الآيـة

بسم الله الرحمن الرحيم

قال تعالي : (قالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ (32)

صدق الله العظيم

البقرة الآية 32

الإهداء

إلى من أرضعتني الحب والحنان إلى رمز الحب وبسلم الشفاء إلى القلب الناصع البياض

والدتي الحبيبة

يا من أحمل اسمك بكل فخر يا من افتقدك منذ الصغر يا من يرتعش قلبي لذكراك

والدي

وإلى كل من جمعتني بهم رحم أمي وكل من جمعتني بهم دور العلم والمعرفة

وإلى كل من يعمل ويناضل من أجل بناء وطن يحترم الكرامة والإنسانية

وإلى كل رفاقي ورفيقاتي المتمسكون بآمل هذا الوطن رغم المشقة

وإلى كل رفاقي ورفيقات دربي الباحثين عند المعرفة والقيم الإنسانية النبيلة

وإلى المناضلين من أجل الحرية والعدل والسلام والديمقراطية

وإلى كل ضحايا الحروب في العالم أجمع

إلى كل من علمني في هذا الكون الذي بذل قصار جهده للإشراف على هذا البحث الدكتورة/ بلقيس عبد العزيز

وإلى كل هؤلاء أهدى البحث جميعاً

Dedication

This work is dedicated to our mother
and father to our family and our tribe
To our teachers, and colleges.
To burn candles that illuminate for others
He ought me to each of the characters .
But above all our
Prophet Mohhamed.

Acknowledgement

Firstly,I knowledge Allah the almighty.

Secondly, I would like to thank Sudan University of Science & Technology.

Thirdly I wish to express my sincere appreciation and gratitude to my supervisor Dr. Balgiss AbdAlazizfor his passion and patience as well as guidance which enormously contributed so much to the completion of this study.

For everyone help me

Thanks

Abstract

We study the fundamental theorem of arithmetic and unique factorization, and we defined the prime power factorization, we give also some the theorem and example t the multiplicate functions. Also we defined the perfect numbers and mersenne and Fermat number. Also we study the mobius inversion formula and the sum of the divisor.

Finally we solving linear congruence, and study the Chinese reminder theorem and the theorems of Fermat and Euler.

Content

CHAPTER ONE
THE FUNDAMENTAL THEOREM
OF ARITHMETIC AND PRIME POWER FACTORIZATION

Prime Factorization:

Definition (1.1):

Prime compositive a positive integer is saidtobe primeincaceit has exactly tow positive divisors.

A positive integer having more than two positive divisors is said to be composite the number 1 is neither prime nor composite .

Example(1.2):

The primes less than 20 are 2,3,5,7,11,13,17 and 19 .

Theorem (1.3):

Suppose$n > 1$ then n can be written as the product of primes

Proof:

If n is prime we are done (we consider a prime to be a product of one prime). Otherwise n must have apositivedivisor, say d other then itself and 1, then $1 < d < n$.

Let $n = dd'$ chearly, $1 < d' < n$ also we now apply the same argument to d and d'as we did ton. This procedure must end since the factors grow smaller at each stop. But it can stop only when each factor has no positive divisors other then 1and itself that is, when each factor is prime.

Lustrationof the proof. Suppose $n = 120$ we know that $120 = 12 \cdot 10$ now $12 = 3 \cdot 4$ and $4 = 2 \cdot 2$ thus $12 = 3 \cdot 2 \cdot 2$ and all these factors are prime. Likewise$10 = 5 \cdot 2$ and 2 and 5 are prime finally.

120=3·2·2·2·5

And 3,2, and 5 are prime.

Comment on the proof: The proof given is convincing because we can see how each step will proceed, even though the number of steps and branches involved will depend on the particular value of n. In this respect, it's like our first proof of theorem (showing that $a \equiv b$ implies $a^n \equiv b^n$) we suspect that amore formal argument using mathematical induction could be given this is the case but a slightly different form of the induction principle must be used.

Let $S(n)$ be a statement involving the positive integer n, suppose .

1. $S(1)$ is true .
2. If for some positive integer k all of S(1), $S(2), \ldots.., S(k)$ are true, Then

$S(k+1)$is true.

Then$S(n)$ is true for all positive integer n.

Comment an induction II. Of course the difference between induction II and the form of induction of section is entirely in condition with inductionII we are allowed to assume not only that$S(k) is\ true$ but also $S(1), S(2) \ldots., S(k-1)$. Since we are allowed to assume more, an induction II proof is actually easier at least from a logical standpoint induction I (which what we will call the principle of section when we want to distinguish between the two forms)is, however, formally simpler and suffices for most proofs.

The reader should study the induction proof we now give for Theorem (1.3) and decide why induction Π is needed in it.

Theorem (1.4):

suppose $n > 1$ is an integer then n can be written as a product of a primes.

Proof:

the proof will be by induction Π

1. If $n = 1$ there is nothing to prove since the theorem concerns only values of n>1.
2. Suppose we know the theorem is true for

$n = 1,2, \ldots, k$consider the integer $k+1$, if $k+1$ is prime then we are done, otherwise $k+1 = dd'$.

Where $1 < d < k + 1$ and $1 < d' < k + 1$since $d$an d' are each at most k by the induction assumption each can be written as a product of primes thus n can be written as such a product.

Thus by introduction Π any $n > 1$ can be written as product of primes.

We will give two more examples of induction Π proofs recall the f_n is the Fibonacci number.

Theorem (1.5):

Let A $= \frac{(\sqrt{5}+1)}{2}$ then $f_{n+2} > A^n$ for all positive integers n.

Proof:

The proof will be by indu

ction Π note that A is a solution to the equation $x^2 - x - 1 = 0$ and so $A + 1 = A^2$

If $n = 1$ we have $f_{n+2} = f_3 = 2 = \frac{3+1}{2} > \frac{\sqrt{5}+1}{2} = A^n$

And so the inequality holds.

We will also check the case $n = 2$ so that we may assume that $k > 1$ in the second port of this proof they

$$x^2 - x - 1 = 0 \text{and so} A + 1 = A^2$$

$$f_{n+2} = f_4 = 3 = \frac{3+3}{3} > \frac{\sqrt{5}+3}{2} = A + 1 = A^2 = A^n$$

Suppose we know for some integer $k > 1$ the inequality holds for

$n = 1,2, \dots\dots, k$. then

$$f(k+1) + 2 = f_{k+2} + 2 + f_{k+1} > A^k + A^{k-1} = A^{k-1}(A+1) = A^{k-1}A^2 = A^{k+1}$$

Thus by induction Π the theorem holds for all positive integer n.

The next result was mentioned in section it justified the “sub situation” of congruent numbers in integral polynomials .

Theorem (1.6):

Let $P(x)$ be polynomial with integer coefficients, and let u, v and $m > 0$ be integer such that $u \equiv v (mod\ m)$. Then $p(u) \equiv P(v)\ (mod\ m)$.

Proof:

If $P(x)$ is constant there is nothing to prove, so we will assume.

$P(x)$has degree $n \geq 1$ suppose $p_{(x)} = a_0 + \ldots + a_n x^n + a_{n-1} x^{n-1}$

Where $a_0, a_1, \ldots, a_n$ are integers with $a_n \neq 0$

The proof will be by induction Π on n .

If $n = 1$, then $P(x) = a_1 x + a_0$ then :

$$a_0 \equiv a_0 \ (modm)$$

$$a_1 \equiv a_1 \ (modm)$$

$$a_1 u \equiv a_1 v \ (modm)$$

$$P(u) = a_1 u + a_0 \equiv a_1 v + a_0 = p_{(v)}(modm).$$

Now assume the statement of the theorem is true for all polynomials with ≤ k suppose $n = k + 1$, so

$$p_{(x)} = a_{k+1} x^{\ k+1} + a_k x^k \ + \cdots + a_0$$

Let $Q_{(x)} = a_k x^k + \cdots + a_0$ now $Q_{(x)}$ is either cues that or has or has degree $\leq k$,so

$$Q(u) = Q(v) \ (mod\ m).$$

Also $u^{k+1} \equiv v^{k+1} + Q(u) \equiv a_{k+1}$ (mod m) as above thus.

$$p_{(u)} = a_{k+1 u^{k+1}} + \ Q(u) \equiv a_{k+1} v^{k+1} + Q(v) = \ P(v)(mod\ m)$$

This proves our result for $n = k + 1$.

Thus by induction Π our theorem holds for integers polynomials of all positive degrees, and so for integral polynomials.

Theorem is very important, but gives only half of the story of factorization into primes to motivate the other half we consider counting the positive divisor of an integer it will turn out its factorization into primes will tell us how to do this.

Definition (1.7): $\boldsymbol{\tau(n)}$

We define $\tau(n)$ to be number of positive divisors of n

Example (1.8):

n	Positive divisor of n	$\tau\ (n)$
1	1	1
2	1 , 2	2
3	1 , 3	2
4	1 , 2 , 4	3
5	1 , 5	2
6	1 , 2 , 3 , 6	4
7	1 , 7	2
8	1 , 2 , 4 , 8	4
9	1 , 3 , 9	3
10	1 , 2 , 5 , 10	4

We will examine the function $\tau(n)$ in more details in the next section.

The fundamental theorem of arithmetic what id $\tau(pq)$?

Recall that $\tau(n)$ de notes the number of positive divisors of n, it is easy enough for us to computer that $\tau(2,3) = 4$, since the positive divisors of 6 are 1,2,3, and 6. In general, if p and q are distinct primes they pq has the divisor i, p, q and ?and so $\tau(pq)$ is at least 4. The reader may feel it is obvious that $\tau(pq)$ is exactly 4. After all what other divisor could pq have?

This is asituation where our familiarity with the integers may be a dis advantage, since it may lead us to assume as true thing that really should be proved it happens to be true that pq has no factors other then those listed but we cannot let intuition and experience substitute for a rigorous proof of this fact as useful as intuitions is in mathematics, there are many instances where it has let to serious errors.

In order to demonstrate should not but too much trust in one's intuition about the integers, we will now present two examples of systems in which certain laws with which familiar do not hold.

Let E be the set of all even positive integers : 2,4,6,8, ...If and be are in E, we say that a divides$b$ in E in case $b = ak$ for some element K in E of course, This parallels the usual definition of divisibility integers for example 1 dose not divide 6 because although $6 = 2 \cdot 3, 3$ is not in E. since 1 is not in E we will have to revise our definition of primality ; but the definition we will give will be equivalent to the previous one in the case of the ordinary integers. We will say that P in E is prime of {cannot be written as the product of two other elements of E greater that 1; for example 1 and 6 are prime in E, but $4 = 2 \cdot 2$ is not the reader may easily check that 10 and 30 are also prime in E thus $60 = 6 \cdot 10$ is of the form pq , where P and q are a district primes .

The integer $60 = 2 \cdot 30$ and 2 is are primes, we have factored 60 into prime factors in two essentially different ways something (it will out) we could never do with the ordinary integers.

Not that the system E is not at all exotic and in fact shores most of the usual algebraic properties of the integers, for example it is closed molar both addition and multiplication. One basic property it lacks is thatof having a multiplicative unit 1 our next example will contain 1 .

Let T bell all positive integers congruent to 1 modules 3; the numbers $1,4\,,7,10,$...since $a \equiv 1(mod\ 3)$ and $6 \equiv b(mod\ 3)$

Imply $ab \equiv 1\ (mod\ 3)$ we see that t is closed under multiplication.

If a and$b$ are in T we say a divided b in T in case $b = ak$ for be written as product of two factors in T greater then 1.

We find the smallest compositive element of T to be $16 = 4 \cdot 4$ and it is easy to check that $4,10,22$ and 55 are all prime element of T.

Another shocker:

These numbers provide an example of no unique prime factorization in T , since $220 = 4 \cdot 55 = 10 \cdot 22$ In fact 220 has the divisor 1,4,10,22,55 and 220 in T, in spite of the fact that 220 is of the form pq for district prime p and q.

The unique factorization property:

Chastened by the above examples we return the ordinary integers to prove a theorem showing that such a aberration do not occur among them.

Theorem (1.9) :

Suppose a and b are integers, P is prime, them p/ab then p/a or p/b

Proof :

Suppose $P \nmid$ a thus, since the only positive divisor of p are p and 1, (a,p) must be 1 thus p/b

This result is the key to showing that the ordinary integers enjoy unique factorization. Suppose the integer $n > 1$ has two factorization in to primes, say $n = P_1P_2 \dots P_s = q_1q_2 \dots q_t$

Since P_1 divides the right side of the last equation theorem(1,8) implies that p_1 divides either $q_1$or$q_2, \dots, q_t$. In the latter case, $P1$ divides either q_2 or the product of the remaining q_s by the same argument eventually we find that $p1$ divides are of the q_s, say q_i But since q_i is prime its only divisors are it self and 1, so we must have $p_1 = q_i$.

Now e divide both sides of the equation by $p_1 = q_i$ and apply the same argument to p_2.Finding that it must equal one of the remaining q_s. We cancel this prime in the same way.

This process is continued as long as possible both sides must be exhausted at the sometime, otherwise we would have a product of primes equaling 1 we have matched each P with a q. Thus the q_s must simply be arrangements of the p_s.

Note that the key to proving unique factorization is theorem (1.8) this result may be found in Book VII of Euclid's elements, stated as follows “if two numbers by multiplying one another make some number, and any prime number measure the product it will also measure one of the original numbers” . The theorem just proved is often combined with the theorem giving the exercise and of a prime factorization as follows:

Theorem (1.10) :(The fundamental theorem of arithmetic)

Any integer n greater than 1 has a factorization in to primes. This factorization is unique to the order of the factors.

The Importance of unique factorization:

The assumption that the factorization of a number in to primes must unique has a famous precedent in mathematical history. Consider the equation:

$$x^n + y^n = z^n x > 0 , y > 0 , z > 0$$

This is an example of a Diophantine equation, that is an equation for which integral (or, sometimes, rational) solution are desired. The name comes from the Greek mathematician diaphanous, who studied many such equating. If $n = 2$, it is easy to final solution to; for example, $x = 3, y = 4 , z = 5,$ or $x = 12, y = 5,$ $z = 13$ for $n > 2$, however, it is a different story. An account of the recent proof by Andrew wiles that no solution exists if $n > 2$ may be found in chapter 0 of this book. The proof settles a problem that goes back more than 200 years.

Around 1637 the French mathematician Pierre de Fermat writing in the margin of his copy of the works of Diaphanous, claimed that he had found “a truly wonderful” proof that had no solution for $n > 2$, nut that there was not room for him to write it down there.

This statement is known as Fermat’s last theorem. If Fermat wrote down his alleged proof anywhere, no one ever found it more than 200 years after Fermat’s claim, interest developed in the connection between Fermat’s last theorem and algebraic integers these are real or complex a numbers that behave like the ordinary integers in many respects in particular, The concepts of divisibility and primarily can be defined in various sets of algebraic integers. The French mathematicians lame and Cauchy through they were close to proofs of Fermat’s last theorem based on the assumption that prime factorization of algebraic integers was unique.

An often-repeated story is that the German mathematician kummer submitted manuscript purporting to contain a proof which was invalid because of this assumption. (Inside many classes of algebraic integers factorization is not unique; the set S that we will define shortly is one example ;) Kummersupposed manuscript has never been found, however, and doubt has been theorem on this part of the story. The interested reader should consult the book by Edwards in the reference.

In any case, kummer went on to prove many important result related to Fermat's last theorem, including the impossibility of for a large number of values of n. His work led the way to the modern theory of algebraic numbers.

The systems:

We define S to be the set of all complex numbers of the form $a + b\sqrt{-6}$

Where a and b are ordinary integers. It is easy to see that S is closed under addition and, sine

$$(a + b\sqrt{-6})\,(c + d\sqrt{-6}) = ac - 6bd + (ad + bc)\sqrt{-6}$$

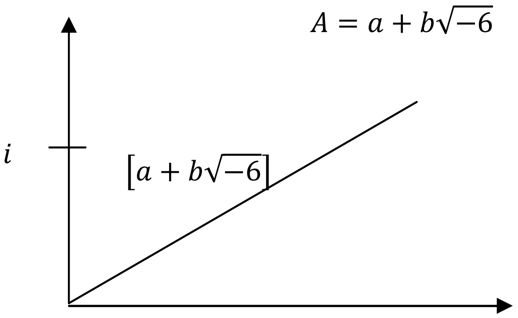


Figure An element of S

Also closed under multiplication.

As usual,if$A$ and B are in Swe say Adivides B in S in case $B = AC$ for some element $C$of$S$. Since the concepts of being positive or negative do not apply to complex numbers, we must modify our definition of primarily. We say p in S is prime in case we cannot write P as a product AB where A and B are in S and neither A nor B is 1 or -1 .

It is perhaps not clear that elements of S can be factored in to primes, since the argument given in section depended on the factors of a number being smaller than the number; while here the factors are complex numbers, to get around this, we consider the square of the modulus (distance from the origin) of an element

$A = a + b\sqrt{-6}$ or s,

given by

$$A = \left|a + b\sqrt{-6}\right|^2 = \left|a + b\sqrt{6i}\right|^2 = a^2 + 6b^2$$

See figure it is not hard to check that

(1) $|A|^2 = 0$ if and only $A = O$

(2) $|A|^2 = 1$ if and only $A = 1$ or $A = 1$

(3) $|AB|^2 = |A|^2|B|^2$

(These and some other details concerning S will be left for the exercise at the end of this section).

Then $|A|^2$ is a nonnegative integer for A in S, and if $c \neq 0, \pm 1$ is not prime in S, then $C = AB$, where

$1 < |A|^2 < |C|^2$and1 $< |B|^2 < |C|^2$

FROM THIS ONE can show using induction Π on $|C|^2$ that any element $|C|$ of S other then 0,1 and -1 has a prime factorization.

We will show that 2 is prime in S, suppose $2 = AB$, where neither A or B is 1 or -1 then .

$$1 = |A|^2|B|^2 = |AB|^2 = |2|^2 = 4$$

By property (3) since $|A|^2$ and $|B|^2$ are both ordinary integer > 1, we must have $|A|^2 = 2\ letA = a + b\sqrt{-6}$ then $a^2 + 6b^2 = 2$ this is impossible whether$b = 0$ or b is not 0a similar proof (depending on the fact that a^2+$6b^2 = 5$is impossible) shows that 5 is prime in S , Another prime in S is $2 + \sqrt{-6}$ for suppose $2 + \sqrt{-6} = AB$ with $1 < |A|^2$ and $1 < |B|^2$ then

$$|A|^2|B|^2 = |AB|^2 = \left|2 + \sqrt{-6}\right|^2 = 2^2 + 6.1^2 = 10$$

By the assumption on $|A|^2$ and $|B|^2$ we must have $|A|^2 = 2$ or $|A|^2 = 5$ But both of these are impossible by previous Calculations, A similar proof shows that $2 - \sqrt{-6}$ is prime in$S$, now observe that

$$\left(2 + \sqrt{-6}\right)\left(2 - \sqrt{-6}\right) = 2^2 - (\sqrt{-6})^2 = 4 - (-6) = 10$$

Thus we have the two distant factorization

$$2 \cdot 5 = (2 + \sqrt{-6)}\,(2 - \sqrt{-6)}$$

Of 10 in to primes in S.

Dividing Exactly:

Now we return to the ordinary integers. Since the factorization of an integer in to primes is unique except for order, the number of times a particular prime appears is determine, justifying the following definition.

Definition (1.11) (divides exactly):

Suppose P is a prime and $k > 0$ we say p^k divides a exactly, and write $p^k||a$, in case $p^k|a$ but $p^{k+1} \nmid a$.

Example (1.12):

$3 \, || \, 6, 2^5 || \, 96, 9 \, || \, 27$is false, $4 \, || \, 24$ is false, $4 \, || \, 62$ is false.

Prime Power Factorization:

The existence and uniqueness of the prime decomposition of an integer are very important for understanding the integers and proving things about them. Thinking about an integer in terms of its prime factorization provides an entry to many number theoretic problems when a proof using prime factorizations works, it is usually straight forward, if not necessarily elegant the next theorem shows how the concepts of divisibility and of the ged and icm depend on prime factorizations.

Theorem (1.13):

Suppose a and b are positive integers, let the distinct primes dividing a or b (or both) be$p_{1,}p_2, \dots, p_{n,}$ suppose.

$$a = p_1^{j_1} p_2^{j_2} \dots p_n^{j_n} \text{ and } p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$

where some of the exponents may be 0, let mi be the smaller and m_iThe larger of $J_i$and k_i for $i = 1,2, \dots, n$ then

(1) $a \mid b$ if and only if $j_i \leq k_i$ for $i = 1,2, \dots, n$.

(2) $(a, b) = p_1^{m1} p_2^{m_2} \dots p_n^{m_n}$.

(3) $[a, b] = p_1^{M1} p_2^{M_2} \dots p_n^{M_n}$.

Proof: (partial)

(1) Suppose $a|b$ then $b = ac$ for some integer$c$. consider the prime factorizations of a, b and c. According to the equation $b = ac$ every prime appearing in the

factorization of a must also appear in that of b, and at least as many times, (here we have used the fact that the factorization is unique up to order) . Thus $j_i \leq k_i$ for all $i.$ Since part (1) contains an "if and only if" statement, this is only half of it its proof we leave the half for the exercises at the end of this section.

(2) Since $mi \leq$ both $j_i$and $k_i$for all i part (1) shows the expression on the right side of (2) to be a common divisor of $a$and b.

Now suppose d is any common divisor of $a$and b, then by part (1) again

$d = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$, where $r_i \leq j_i$and $r_i \leq k_i$

For all i. Then $r_i \leq m_i$ for all i and so d is less than or equal to the right side of (2).Thus the right side of (2) is a common divisor of a and t exceeding any other common divisor. By definition it is (a, b) .

(3) This proof is left for the problems.

Example (1.14):

(of the use of theorem (1,12) suppose $a = 75 = 3^1 5^1, b = 900 = 2^2 3^2 5^2$and c = 400 = $2^3 5^1 11^1$ then :

(1) $a|b$ since $a = 2^0 3^1 5^2$. And $0 \leq 2, 1 \leq 2$ and $2 \leq 2$;

(2) $(b, c) = 2^2 3^0 5^1 11^0 = 20;$

(3) $[b, c] = 2^3 3^2 5^2 11^1 = 19{,}800$

Factoring large numbers:

Using part (2) of the last theorem appears to be easier thanusing the Education algorithm. This method depends on knowing the prime factorization of the numbers involved, however. If n has mostly small prime factorization of many befound by dividing through by each factor as it is found. If n has only large prime divisors, however. Finding they may be difficult. In such a case the Education algorithm and the equation $[a, b] = |ab|/(a, b)$ will still provide the easiest way to find the gcd and ICM of two numbers very often the digits of a number tell us something about its divisor for example, we know the number 7,586,634 is even without bothering to divide it by 2- because its last digit is even this idea is so familiar that we have probably never thought about why it is ture writing out a formal proof may be instructive.

Proposition (1. 15):

A positive integers written to base 10 is even if and only if its last digit is even.

Proof:

Suppose n has the digits $a_k a_{k-1}, ..., a_0$ starting from the left

So $n = a_k 10^{\mathrm{k}} + \cdots + a_1 10^1 + a_0$

We want to show that n and $a_0$are either both even or both odd another way to say this is that .

$$n \equiv a_0 (mod 2)$$

But this is implied by the fact that 10 ≡ 0(mod2) and what we know about manipulating congruence's.

Prosperities of digits:

The key to the proof just given is the fact that$10 \equiv 0(mod 2)$, and we write numbersin terms of powers of 10 (no doubt because humans have 10 figures).

If a different base were used the theorem might not be true, similar theorems can be proved for other divisors d, provided, that 10 is sufficiently simple modulo. for example. The same proof shows that a number is divisible by 5 if and only if its last digit is actually, the proof says even more, namely, that apositive integers is congruent module 5 to its last digit. Thus we can say not only that $38,707$ is not divisible by 5, but also that its east residue module 5 is 2 since this is true for7.

A similar proof shows that a positive integer is congruent to the sum of its digits modulo both 3 and 9 in particular n is divisible 3(or a) if and only if the sum of its digits is. We will do the proof only for3.

Proposition (1.16):

Any positive integer is congruent to the sum of its digits module 3.

Proof:

Let $n = a_0 + \cdots + a_k 10^k$ note that $10 \equiv 1(mod\ 3)$.Then

$$n \equiv a_k(1)^k + \cdots + a_1\ (1) + a_0(mod3).$$

A similar theorem holds for the modules 11 we omit the proof.

Proposition (1.17):

In $n = a_k 10^k + \cdots + a_0$then.

$$n \equiv a_0 - a_1 + a_2 \ldots\ (mod\ 11)$$

the following summarizes our results on digits .

Theorem (1.18): (The digit theorem):

Let $n\ > 0$ have the decimal representation $a_k a_{k-1} \ldots a_0$then:

(1)$n\ \equiv\ a_0(mod\ 2)$.

(2)$n\ \equiv\ a_0(mod\ 5)$.

(3)$n\ \equiv\ a_k\ +\ \ldots\ldots\ldots\ldots\ldots\ldots + a_0(mod\ 3)$.

(4)$n\ \equiv\ a_k\ +\ \ldots\ldots\ldots\ldots\ldots\ldots +\ a_0(mod\ 9)$.

(5)$n\ \equiv\ a_0 -\ a_1 + \cdots + \cdots\ a_0\ (mod\ 11)$.

Example (1.19):

We will factor $n =\ 37{,}719$ since $3 + 7 + 7 + 1 + 9\ =\ 27$, we see $9|n$ ln. Division produces $n\ =\ 9{,}4191$. Now we concentrate on 4191. Since $4 + 1 + 9 + 1\ =\ 15, 41\ 91$ is divisible by3 but not 9 a we have $4191\ =\ 3.1397$.

Ordinary divisionshows $7 \nmid 1397$. The next prime is 11 since 11 doesn't divide $7 - 9 + 3 - 1$, we go on to 13.

Now $13^2 =\ 169$, so $127/13\ < 13$. Thus if 127 had a proper factor $\geq\ 13$, then it would also have a factor < 13. Since the latter possibility has been eliminated, we conclude that 127 is a prime .thus $37{,}719\ =\ 3^2\ \ 11.127$.

Theorem (1.20):

If the integer $n\ > 1$ has no prime divisor $\leq\ \sqrt{n}$, then n is prime .

Proof:

This proof is illustrated by the argument about 13 at the end of the last example , Suppose n is compositie . then $n\ =\ d_1 d_2$ where both d_1 and d_2 exceed if booth

d_1 and d_2 exceed $\sqrt{n}$ then $n = d_1 d_2 > \left(\sqrt{2}\right)^2 = n,$ Which is impossible suppose $d_1 \leq \sqrt{n}$, then d_1 is either prime or else has a prime divisor $\leq \sqrt{n}$.

The set of Primes in Infinite:

Suppose we want to determine all the primes less than 100. We might proceed as follows. First we write out the integers from 2 to 100. We know 2 isprime; let us circle it and cross out the remaining even numbers on our list. Now the lowest number that hasn't been crossed out is 3; we circle it and cross out ever third number thereafter, since 3 is a proper divisor of each of these our list now starts as follows:

② ③ 5 7 11 13 17……………………..

At each stage in this procedure the smallest number that has not been circled or crossed out must be prime. since otherwise it would have a smaller prime divisor, and so have been eliminated already .

This process is called the sieve of Eratosthenes, after the Greek scientism who invented it, note that according to Theorem (1.19) in order to find all the primes up to n we need only sieve out multiples of primes $\leq \sqrt{n}$ to find the primes up to 100, for example, we need only cross out multiples, of 2,3,5 and 7 the operation of the sieve of Eratosthenes, suggests that primes should be rarer among the larger integers. For example , it's application to the numbers between 100 and 150 consists in crossing out the multiples of the 5 primes 2,3,57 and not exceeding $\sqrt{150} \approx 12.2$ Applying the sieve between 1000 and 1050 however, we eliminate not only the multiples of all these primes, but also the multiplies of the additional 6 primes 13,17,19,23,29 and 31 between 12.2 and $\sqrt{1050} \approx 32.4$ it turns out that there are 10 primes between 100 and 150 but only 8 between 1000 and 1050 between 10,000 and 10,050 , there are just 4 primes .

These considerations suggest the possibility that at some stage in the application of the sieve all longer numbers will have been crossed out so there would be no more primes. This would mean that there would exist only finitely many primes, say $p_1, p_2, \dots, p_k$ so that each integer greater then 1 could be written as a product of powers of these primes. The integers

$$p - p_1 p_2 \dots \dots \dots . . p_k$$

would then have the interesting property that $(p, n) > 1$ when even $n > 1$, since all the distinct prime factors of n would appear in p.let us make atable of (p, n) for small values of n.

n	1	2	3	4	5	6	7	8	9	10
(p, n)	1	2	3	2	5	6	7	2	3	10

Back in section we made a similar table for$(6, n)$ it turned out to be periodic, with period 6. In fact we proved in theorem that if $b \equiv b' \ (mod\ a)$,then $(a, b) = (a, b')$. But this doesn't square with what we know about (p, n) says that if $n \equiv 1(\ mod\ p)$. Then $(p, n) = (p, 1)$; for example $(p, p + 1) = 1$ our definition of p, however, led us to the conclusion that $(p, n) > 1$ for $n > 1$, The trouble must be in our assumption that the number of primes is finite , which has produced a contribution thus we have proved the following theorem.

Theorem (1.21):

The number of prime is infinite.

Euclid's proof that the number of primes is infinite:

Theorem first appears in the works of Euclid, so we will give his proof, which has the advantage of depending on little beyond the definition of the primes. As before we assume there are only the primes $p_1 p_2 \dots \dots \dots . . p_k$ and more consider the number $Q = p_1 p_2 \dots \dots \dots . . p_k + 1$

Now Q is either prime or else has a prime factor, If Q is prime we have a contradiction, since $p_1 p_2 \dots \dots \dots . . p_k$ are supposed to be all the primes, But any prime factor of Q must be different from all of $p_1 p_2 \dots \dots \dots . . p_k$, since It is easy to see that none of the ps can divide Q. This again contradicts the assumption that $p_1 p_2 \dots \dots \dots . . p_k$ comprise all the primes.

Now we give a more sophisticated proof of Theorem by the Swiss mathematician Leonhard Euler some exposure to infinite series is desirable (but not absolutely necessary) for it'sunderstanding Again we assume

$p_1p_2 \ldots\ldots\ldots.., p_k$are all the primes, Then if n is any positive integer wemay choose r big enough so that all the terms $1,$ ½, ⅓ , $\ldots\ldots\ldots\ldots..\, {}^{1}/_{n}$ appear when

we multiply out the product .

$$\left(\mathbf{1}+\frac{\mathbf{1}}{\boldsymbol{p_1}}+\frac{\mathbf{1}}{\boldsymbol{p_1^2}}+\ldots.+\frac{\mathbf{1}}{\boldsymbol{p_1^r}}\right)\left(\mathbf{1}+\frac{\mathbf{1}}{\boldsymbol{p_2}}+\frac{\mathbf{1}}{\boldsymbol{p_2^2}}+\ldots.+\frac{\mathbf{1}}{\boldsymbol{p_2^r}}\right)\ldots\ldots\left(\mathbf{1}+\frac{\mathbf{1}}{\boldsymbol{p_k}}+\frac{\mathbf{1}}{\boldsymbol{p_k^2}}+\ldots..+\frac{\mathbf{1}}{\boldsymbol{p_k^r}}\right)$$

In fact increasing r merely adds in more terms for example we get ${}^{1}/_{12}$ by choosing $1/\,2_2$ from the first factor. ⅓ from the second, and 1 from all the others (assuming that$p_1 = 2$ and $p_2 = \ 3)$.

Now by the formula for the sum of a geometric progression

$$1+\frac{1}{p_1}+\frac{1}{p_2}+\ldots.+\frac{1}{p^r}=\frac{1-(p^{1-})^{r+1}}{1-p^{-1}}<\frac{1}{1-p^{-1}}=\frac{p}{p-1}$$

We see that for any n the sum

$$1+\frac{1}{2}+\frac{1}{3}+\ldots.+\frac{1}{n}$$

Cannot exceed

$$\frac{p_1}{p_{1-1}}.\frac{p_2}{p_{2-1}}\ldots\frac{p_k}{p_{k-1}}$$

But this contradicts the divergence of the harmonic $1+\frac{1}{2}+\frac{1}{3}\ldots\ldots\ldots.$

(to get the contradiction without knowing about the harmonic series, see problem 20 at the end of this section)

The distribution of prime has been studied extensively and is a central topic in what is known as analytic number theory unfortunately what can be proved mostly involves techniques too advanced to be presented here. The prime number theorem which was proved independently n 1896 by Hadamard and de la vallěě - pousin, states that .

$$\frac{\pi(x)}{x/\log_e x}\rightarrow 1\ as\ x\ \rightarrow\infty$$

Where $\pi(x)$ is the number of primes $\leq\ x$.

There is a scarcity of result implying the expense of infinitely many primes of special forms for examples primes p and q are called twin primes if they differ by

2 Example are 3 and 5,5 and $7, 11$ and 13 and 41 and 43 and $1,000,000,009,64$ 9 and $1,000,000,009,651$. When a list of large primes is complied, twin primes appear to continue to pop up no matter how for out one goes, but the twin prime conjecture, which states that there are infinitely many of them, has never been proved.

The one positive result of this type is Dirichlet's theorem, which says that if a and b are relatively prime, then the infinite arithmetic progression $a, a+b, a+2b, \dots..$ contains infinitely many primes.

Before the development of electronic computers mechanical devices were constructed to perform tedious number – theoretic computations. figure 2.2 shows a photograph of machine made by DrH. Limber of the university of California such devices played an important part in primality testing and factorization before the birth of modem computers.

We now return to the evaluation of $\tau(n)$, which was sidetracked when we get into much more interesting problem of prime factorization. What we know now makes the problem easy suppose.

$n = p_1^{k_1} p_1^{k_2} \dots \dots \dots .. p_1^{kt}$,

Where the ps are distinct primes. If d is appositive divisor of n, then by the first part of Theorem (1.4)

$$d = p_1^{j_1} p_2^{j_2} \dots \dots \dots .. p_t^{j_t}$$

Where $0 \le j_i \le k_i$ for $i = 1,2 \dots \dots, t$.

(we allow the j_s to equal 0 to take of care of primes not dividing d at all).

Example (1.22):

If $n = 63 = 3^2 7$, then the positive divisors of n are

$$3^0 7^0 3^1 7^0 3^2 7^0$$

$$3^0 7^1 3^1 7^1 3^2 7^1$$

Returning to the general case, we note that the unique factorization theorem also tells us that each different choice for j_1 through j_t gives us a different d, since there are $k_1 + 1$ possibilities for $j_1$namely $(0,1, \ldots\ k_1)$, $k_2 + 1$ possibilities for j_2, etc. we have the following theorem.

Theorem (1.23):

If $n\ = p_1^{k_1}p_2^{k_2} \ldots . p_t^{k_t}$, where $p_1, p_2, \ldots, p_t$ are distinct primes .

Then:

τ(n) = $(k_1 + 1)\ \ (k_2 + 1) \ldots \ldots \ldots \ldots .. (k_t\ + 1)$

Example (1.24):

Since

$$63\ = 3^2 7\,,\ \text{wehave}\ \ \tau(63) = (2+1)(1+1) = 6$$

Likewise

$$\tau(120)\ =\ \tau(2^3 3^1 5^1)\ =\ (3+1)\,(1+1)\,(1+1)\ =\ 16$$

Writing divisor in a multiplication table:

When before the theorem, we wrote out the positive divisors of 63, we found it convenient to organize then into a rectangular array. This array may have reminded the reader of a multiplication table, indeed, that is exactly what it was. Let us look at it again.

	1	3	9
1	1	3	9
7	7	21	63

We have written the positive divisor of 9 along the top and those of 7 along the left side. Each entry in the table is the product of a divisor of a and one of 7 thus in this case

$$\tau(63)\ =\ \tau(9)\tau(3)\ =\ 3.2\ =\ 6$$

This suggests that we might prove in general tat $\tau(ab) = \tau(a)\tau(b)$ by showing that the divisors of are just all products of a divisor of a with one of b.

Let us suppose a and b have the positive divisors $d_1, d_2, \ldots d_s$ and $e_1 \ldots, e_t$, respectively. Thus $\tau(a)\ = s$ and $\tau(b)\ = t$

We consider the array

d_1e_1 d_2e_1 ,…………….d_se_1
d_1e_2 d_2e_2 ,…………….d_se_2
d_1e_t d_1e_t ,…………….d_se_t

This array has st entries, so in order to show τ(ab) =st we must demonstrate three things:

(i) Every entry is divisor of $a\ b$.

(ii) Every positive divisor of ab appears in the array.

(iii) No two entries are equal.

Since (i) is easy to see we proceed (ii). Suppose c is a positive divisor of ab .then there exists an in integer K such that $=\ ck$. Consider the prime factorizations of both sides of this equation. By the fundamental theorem of arithmetic e can match up the primes in both sides in one-to one fashion in particular, some of the primes in the factorization of c match up with primes in the factorization of a, and the rest with primes in b. We see that c is a product of a divisor of with one of b.

We now turn to condition (iii). Suppose that two entries of the array are equal say $d_ie_j =\ d_ke_i$. If we know that the prime factors of d_i could only occur in d_k,And vice versa we could conclude that $d_i\ =\ d_k$ and $e_j = e_i$ would follow unfortunately. This need not be true. For example. The primes dividing both a and b.Then p. 1 and $1.p$ will appear at different places in the array.

Evidently we need an additional hypothecs in order to prove (iii) namely , that no prime divides both a and b . If this is the case, we easily see that $d_ie_j = d_ke_l$ implies that $d_i = d_k$ and $e_j = e_l$, since , for example, the primes dividing $d_i$cannot appear in e_i adivisor of b, and so must all turn up in $d_k$since saying no prime divides both a and b is equivalent to saying (a, b) =1 we have proved the following theorem.

Theorem (1.25):

If a and b are relatively prime positive integer, then: $\tau(ab)\ =\ \tau\ (a)\ \tau\ (b)$.

The analysis above involves a more specific discovery that will be used again.

Theorem (1.26):

If a and b are relatively prime possessive integers, then the set of positive divisor of ab consists exactly of all products de, where d is a positive divisor of a and e is a positive divisor of b , furthermore, these products are all distinct.

Definition (1.27):

Numerical function $f(n)$ is said to be multiplicative if

$$f(a\ b) = f(a)f\ (b)\text{whenever } (a, t) = 1$$

CHAPTER TWO
NUMERICAL FUNCTIONS

Functions the like $\tau(n)$ the number of positive divisor,of n, defined on the positive integers, are variously called numerical arithmetic, or number- theoretic functions. They are treated in this chapter.

The sum of the Divisor:

Definition $\sigma(n)$ (2.1):

Let n be a positive integer, we define $\sigma(n)$ to be the sum of the positive divisor of n .

Example (2.2):

Let $n = 7$ we have $\sigma(n) = 1 + 7 = 8$; for n=9 we have $\sigma(n) - 1 + 3 + 9 = 13$, and for $n = 63$ we have $\sigma(n) = 1 + 3 + 9 + 7 + 21 + 63 = 104$

The astute reader may have noticed the $\sigma(63) = 104 = \sigma(7)\,\sigma(9)$, and that in fact in addingup the positive divisors of 7 times those of 9 were seeing a repetition of the ideas leading to our proof the $\tau(n)$ was multiplication table of the divisors of 7 times those of 9 were seeing a repetition of the ideas leading to our proof the $\tau(n)$ was multiplicative Indeed, in last section may be wed to prove $\sigma(n)$ multiplicative just as it was used to prove $\tau(n)$ multiplicative. The reader may want to try to provide his or her own proof for the next theorem before reading the one given.

Theorem (2.3):

The function $\sigma(n)$ is multiplicative .

Proof:

Suppose a and b are relatively prime positive integers let the positive divisor of a b c $d_1 d_2 \ldots, d_s$ and let these of b be $e_1, e_2 \ldots, e_t$ then :

$$\begin{aligned} \sigma(a)\,\sigma(b) &= (d_1 + d_2 \ldots\ldots + d_s)\,(e_1 + e_2 \ldots\ldots\ldots\ldots.. + e_t) \\ &= (d_1 e_1 + d_2 e_2 \ldots\ldots\ldots\ldots\ldots.. + d_s e_1) \\ &= (d_1 e_2 + d_2 e_2 \ldots\ldots\ldots\ldots\ldots.. + d_s e_2) \end{aligned}$$

$$+\ (d_1e_t + d_2e_t \ldots\ldots\ldots\ldots\ldots.. + d_se_t)$$

But the numbers in this sum are exactly the positive divisor of ab . Thus $\sigma(a)\sigma(6) = \sigma\ (ab)$.

The summation nutrition:

There is a note ration for sum that avoids the sprawl (and possible ambiguity) of the $s..$ used above. The Greek letter $\sum$(capital sigmats) signals the sum of terms each of which depends on integers that varies between two limits, for example thesum.

$$= \ d_1 + d_2 + \cdots + d_s$$

Of the interest in the last theorem would be expressed as

$$\sum_{l=1}^{s} di$$

ingeneral, if f is some function of an integral variable and $m \leq n$ by

$$\sum_{l=m}^{n} f(i)$$

We mean

$$f(m) + f(m+1) + f(m+2) + \cdots + f(n)$$

The viable i is called the index of summation and is similar to the variable of integration in s definite integral in that it really does not matter what matter is used.

For example

$$\sum_{i=1}^{5} i \ and \ \sum_{5=1}^{5} j$$

bother man the something(inemely,15) end any other letter could be used in place of i or$j$ soling as it had no previous meaning.

In number theory, it is common to extend the summation notation to situations in which the index of summation does not run through a set of consecutive integers.

A description of the values the index is allowed to assume is simply written under the. For example,

$$\sum_{\substack{p\ prime \\ p<7}} p^2 = 4 + 9 + 25 = 38,$$

And

$$\sigma_{(n)} = \sum_{\substack{d|n \\ d>0}} d.$$

To interpret the last summation. Correctly the reader must realize that d and not n the index of summations (in $\sigma_{(n)}$), something an indexof summation never does. When summing over the divisor of anumber we generally wish to consider those that are positive (so in order to avoid always writing $d > 0$under the sigma we establish the following convention when assumption is over the divisor of a number theses divisor are restricted to be positive.

There are various rules for manipulating summations that follow from the usual rules of algebra for example.

$$\sum_{l=1}^{n} k\, f(i) = k \sum_{l=1}^{n} f(i)$$

Because

$$kf(1) + \ kf(2) + \ ... + k\, f(n) = \ k\big(f(1) + \cdots + f(n)\big)$$

According to the distributive low. Similar rules will be found in the exercise and can be proved by reverting to the notation.

One way to express the number of elements in a set is to sum 1 over that set for example.

$$\tau(n) = \sum_{d/n} 1$$

Knowing that a function is multiplicative is valuable necuasse it reduces the problem of determining a formula to evaluation at a power of a prime. Suppose, for example,

$$n = p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}$$

where the p_s are distinct prime, and suppose we know of is a multiplicative function.

Then:

$$\text{f}(n) \; = \; f(p_1^{k_1} p_2^{k_2} \ldots p_m^{k_m}) = \; f(p_1^{k_1})\, f(p_2^{k_n} \ldots p_m^{k_m})$$

$$= f(p_1^{k_1})\, f(p_2^{k_2})\, f(p_3^{k_3}) \ldots f(p_m^{k_m})$$

$$= f(p_1^{k_1})\, f(p_2^{k_2}) \ldots f(p_m^{k_m})$$

Evaluating of a prime power is generally simpler then at an arbitrary integer for example.

$$\sigma(p^k) = \; 1 + p + p^2 + \cdots .. + p^k$$

This is a geometric progression, and by the formula we developed in section it is sum is

$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$$

We are now in a position to give a formula for the function σ(n)m but the notation we have would again involve an excessive use of ellipsis (three dots). We need a compact symbolism for products to the sigma notation for sums.

The symbol Π (capital Greek letter pi) is used to denote a product. Thus

$$\prod_{l=1}^{n} f(i) = f(1)f(2) \ldots f(n);$$

and, more generally, if $s(i)$ is a statement about I, by

$$\prod_{s(i)} f(i)$$

wean the product of the numbers $f(i)$ over all valued of I for which $s(i)$ is true

Example (2.4):

$$\prod_{l=1}^{3} i^2 = 1.4.9 = 36 \quad and \quad \prod_{\substack{p\ prim \\ p<5}} \frac{1}{p} = \frac{1}{2} . \frac{1}{3} = \frac{1}{6}$$

And

$$\prod_{l=1}^{n} i = n!$$

The following theorem follows from the fact that a is multiplicative and equation (2.1) above.

Theorem (2.5):

If $n = p_1^{k_1} p_2^{k_2} \ldots \ldots p_m^{k_m}$ where the p_s are distinct primes then:

$$\sigma(n) = \prod_{i=1}^{m} \frac{{p_i}^{k_i+1} - 1}{p_i - 1}$$

Example (2.6):

In $n = 63 = 7.3^2$then:

$$\sigma(n) = \frac{7^2 - 1}{7 - 1} . \frac{3^3 - 1}{3 - 1} . = \left(\frac{48}{6}\right)\left(\frac{26}{2}\right) = 8.13 = 104$$

Likewise:

$$\sigma(1{,}000{,}000) \ = \ \sigma(2^6 5^6) \ = \ \frac{2^7 - 1}{2 - 1} \ = \ \frac{5^7 - 1}{5 - 1} = \left(\frac{127}{1}\right) . \left(\frac{78.124}{4}\right)$$

$$= 2{,}480{,}4327$$

Multiplicative functions:

Manufacturing multiplicative functions;

In the last two sections, we proved first $\tau(n)$ and then $\sigma(n)$ to be in multiplicative, using almost the same proof.

In the last problem set, the functions $s_2(n)$ and $s_{-1}(n)$ were defined to be respectively the sum of the squares and reciprocals of the positive divisors of n, and these both turned out to be multiplicative also let us see how far this method of proofcan be carried. Let us suppose that f is some arbitrary numerical function, and define the function F by

$$F(n) = \sum_{d/n} f(d)$$

asbefore, let us assume that a and b are relating prime, with positive devisors

$d_1 d_2 \dots d_s$and$e_1 e_2 \dots e_t$respectively. Then

$$f(a)f(b) = (f(d_1) + \cdots + f(ds))\,(f(e_1) + \cdots + f(e_t))$$

$$= f(d_1)f(e_1) \dots + f(ds)\,(f(e_1)$$

$$+f(d_1)f(e_2) \dots + f(ds)\,(f(e_2)$$

$$+ f(d_1)f(e_t) \dots f(ds)\,(f(e_t)$$

On the other hand by Theorem (1.25) $f(ab)$ is

$$\big(f(d_1 e_1)\big) + \cdots + f\ (d_s e_t)$$

We see that in order for these two expression to be equal, it is enough that $f(d)f(e) = f(de)$when ever d/a and e/b since in such circumstances d and$e$ will be relatively prime if a and b are, it suffices that the function f be multiplicative in order that F be.

Theorem (2.7):

Suppose f is a multiplicative function, and define F by

$$f(n) = \sum_{d/n} f(d)$$

Then $F$is multiplicative also:

Example (2.8):

Since the function defined by $f(n) = n$ for all n is easily seen to be multiplicative, then so is

$$\sigma(n) = \sum_{d/n} f(d) = \sum_{d/n} d$$

In fact, if we define $f(n) to\ be\ n^k$, we easily see multiplicative thus so is:

$$s_k n = \sum_{d/n} f(d) = \sum_{d/n} d^k$$

Thus at one swop we have shown $\sigma(n)$ (taking $k = 1$), $\tau(n)$ (taking $k = 0$), and the functions of the problems in the last section (with $k = 2$ and -1) to be multiplicative. We now have a general scheme for inventing and finding formulas for multiplicative function of the from

$$f(n) = \sum_{d/n} f(d).$$

We start some simple function F that we prove to be multiplicative. Then by the last theorem F is also multiplicative function) it suffices to evaluate F at prime powers, just as in our derivation of the formula for in section 3.1. As example, we consider the function $g(n)$ defined to be o if n is even and 1 if n is odd.

This is easily seen to be multiplicative since $g(ab)$ and $g(x)\ g(b)$ are both 1 if and only if a and b are both odd.

Now let

$$G(n) = \sum_{d/n} g(d).$$

Then G is multiplicative by the last theorem we evaluate G at prime powers. The prime 2 is a special case.

We have

$$G(2^k) = g(1)\ +\ g(2)\ + \cdots +\ g(2^k) =\ 1 + 0 + 0 + \cdots + 0 = 1$$

On the other hand, if P is odd prime, Then

$$G(p^k) = g(1)\ + g(p)\ + \cdots + g(2)^k\ =\ 1 + 1 + \cdots + 1 =\ k + 1.$$

We see that if $n = 2^k p_1^{k_1} p_2^{k_2} \dots\dots\dots\dots\dots.p_s^{k_s}$, where the$p_s$ are distinct odd primes, Then $g(n) = (k_1 + 1) = (k_2 + 1) \dots\dots\dots\dots. = (k_s + 1)$.

This is similar to the formula for $\tau(n)$. In fact $G(n)$ is the number of odd divisor of n..

The uniqueness of f since Theorem (2.3) is convenient for proving a function to be multiplicative we might wonder, given a function F, if could find a function f such that for all positive integers n.

$$F(n) = \sum_{d/n} f(d)$$

This question will be settled in olives with sawing that if such a function f exists, Then it is unique and in the processes give another example often induction 11 proof.

Theorem (2.9):

Suppose f is a numerical function. Then there is at most one function f such that

$$F(n) = \sum_{d/n} f(d)$$

For all positive integer n. We will show by induction.

If on n that f$(n) = g(n), n = 1,2$ ...

i- Taking $n = 1$ in (2.2) and (2.3) we see that $F(1) = F(1)$,and $F(1) = g(1)$, so $f(n) = g(n)$ for $n = 1$.

ii- suppose for some integer k we have $f(n) = g(n)$ for $n = 1$ suppose for some $n = 1,2, \dots, n$ then

$$f(k+1) = \sum_{d/k+1} f(d) = \sum_{d/k+1} g(d)$$

by the induction hypothesis the two sums on the right have all their teams equal except possibly $F(k+1)$ and $g(K+1)$, which must therefore also he equal.

Thus by the induction II principle we see $F(n) = g(n)$ for all positive integer n.

Why study number theory? Perhaps the reader is wondering what good a function like $\sigma(n)$ is. Who carries that we have found a formula for the sum offline positive divisors of n? This is equation that each person must answer for himself or herself, since number theory, like mountain climbing, is e_1 endeavor practiced mainly just for its own sake. Among the reasons some people might care about it areaccomplishment. Solving a mathematical problem may give the same pleasant feeling problem may give the same pleasant feeling of success finishing a difficult crossword puzzle or writing set of tennis understanding. Knowing why a number is divisible by g if and only if the sum of its digits is I and thus the justification of the old check of “casting on gs” may bring satisfaction.

Skill. A person might take pride in being able to play the quitter or a termski, or just as well , cannot the divisors if million in a few seconds or compute the greatest common divisor if two large numbers.

Beauty many find beauty in number theory, either in the structure of the integers themselves (as an astronomer might find beauty in the hours of the universe), or in an ingenious of elegant proof.

We do or leave the impression that there are no applications at all number theories. The RSA method of public key cryptography, which is treated in section involves many number. Theoretic concepts, and has gained a great deal of attention in recent years. It security depends on the difficulty of factory large numbers, a problem that has been. Studied for centuries. Long before its connection to anything useful. This is similar to man upsides in science in which phenomena studied purely for their theoretical interest later turned out to have immense practical consequences (such as atomic energy).

The study of numbers for their own sake is by no means now. The Greeks, were interested in numbers like 6. This is sum of its positive divisors other than itself, $6 = 1 + 2 + 3$, if n any number with this property. Then $n = \sigma(n) - n$ since by definition $\sigma(n)$ adds in the divisor n itself.

Definition: perfect number (2.10):

We say n is a perfect number in case $\sigma(n) = 2n$.

A table for $\sigma(n)$:

To look for perfect numbers other than 6 we will make a table if the first 30 values of $\sigma(n)$ as follows:

n	$\sigma(n)$	n	$\sigma(n)$	n	$\sigma(n)$
1	1	11	12	21	32
2	3	12	28	22	36
3	4	13	14	23	24
4	7	14	24	24	60
5	6	15	24	25	31
6	12	16	31	26	42
7	8	17	18	27	40
8	15	18	39	28	56
9	13	19	20	29	30
10	18	20	42	30	72

Construction of the table was simplified by using a few properties of $\sigma(n)$.The primes were easily filled in since $\sigma(p) = p + 1$ prime powers follow the rule that $\sigma(p^k) = \sigma(p^{k-1}) + p^k$. Thus $\sigma(4) = \sigma(2) + 4\sigma(8) = \sigma(4) + 8$, etc. the remaining values were then determined by the fact that σ(n)is multiplicative for example, $\sigma(18) = \sigma(2)\,\sigma(9) = 39$, But $\sigma(3)\,\sigma\,(6) = 48$. What's wrong?) interest in perfect numbers precedes Euclid, and many early writers made note of then saint Augustine said that God created the world in six days rather than all at once because "The perfection of the work is signified by the perfect number 6″ others asserted that there are infinitely many perfect numbers; that indeed, there is exactly one between 1 and 10, another 10 and 100, another between 100 and 1000, etc, That all perfect numbers, are even and that the perfect numbers alternately and, in the digits, 6 and 8, none of these assertions has ever been proved, and some are known to be false, we will continue the study of perfect numbers in the next section.

A number is said to be abundant if the sum of the positive divisors of the number other than itself exceeds the number (so $\sigma(n) > 2n$, and deficient if this sum is less than the number (so $\sigma(n) < 2n$.

Example (2.11):

Since $\sigma(12) = 28 > 2.12$. The number 12 is abundant since $\sigma(11) = 12 < 2.11$,. The number. It is deficient, Clearly each positive integer is either perfect, abundant, ore deficient.

We say a pair of numbers a and b is amicable if the sum of the positive divisors of a less than $a$equals b, and the sum of the positive divisors of b less than b equals a. Another's way to way this is that $\sigma(a) - a = b$ and $\sigma(b) - b = a$.

Example (2.12) :

The smallest pair of amicable numbers is 220 and 2,84 here $220 = 2^2 5.11$ and

$\sigma(220) - 220 = \sigma(2^2)\sigma(5)\sigma(11) - 220$=$7.6.12 - 220 = 284$

$$\text{Likewise } 284 = 2^2 71$$

and

$$\sigma(284) - 284 = \sigma(2^2)\sigma(71) - 284 = 7.72 - 284 = 220$$

Amicable primes have long been considered important in numerology (which has the same relation to number theory as astrology to astronomy). The following is from the writings of the Arab scholar IbnKhaldun $(1332-1406)$: Let us mention that the practice of the art of talisman has also made us recognize thatmarvelous virtues of amicable (or sympathetic) numbers. These numbers are 220 and 248. One calls them amicable because the aliquot parts of one when added give assume equal to the other persons who occupy themselves with talismans assure that these numbers have a particular influence in establishing union and friendship between two individuals. One prepares a horoscope theme for each individual, the first under the sign of venues while it presents in regard to the moon an aspect of love and benevolence. In the second theme the ascendant should be in the seventh sign. On each one of these themes one inscribes one of the numbers just indicated but giving the strongest number to the person whose friendship one wishes to gain the beloved person, I don't know if by the strangest number one wishes greatest number of aliquot parts. There results a bond so between the two people they cannot be separated. The author of the chain and other great masters in this art declare that they have seen this confirmed by experience.

The pair 220,284 was the only one known to the ancients, and it was not until 1636 that another pair was found by Fermat, now about 400 pairs of amicable numbers are known,In 1866 a sixteen-year-old Italian boy, Nicola Paging. Found the pair 1184, 1210, which had been over looked by mathematicians up to that time. Incredibly, only 220, 284 are smaller. At a meeting of the American mathematical society in San Francisco in 1983 Hilton Chen and Dale woods of NorthjeastMissouristate University announced two previously unpolished pairs of amicable numbers, The larger of which was

$$A = 21,741,269,040,875,083,566,772,572567,93.5,979,368,836,363,843$$

$$B = 22,261,723,990,815,556,829,012,769686,652,975,057,619,942,956,477$$

Perfect Numbers:

Looking for a pattern; So for we have found only two perfect numbers, 6 and 28 let us computer $\sigma((n)$ for each of these to try to see why it equals 2n.

$$\begin{tikzcd}[column sep=small]
(6) = (2 \arrow[r, bend left] & 3) = (2) \arrow[r, bend left] & (3) = 3 & 4 \\
(28) = (4 \arrow[rr, bend left] & 7) = (4) \arrow[rr, bend left] & (7) \ =7 & 8
\end{tikzcd}$$

Each of the perfect numbers we know consists of a power of 1 times a prime as the arrows indicate, when we apply σ to each, the power of 2 turns on to the prime and the prime turns in to twice the power of 2. What must the relation between the prime and the power of two before this work?

Suppose $n = 2^r p$, where p is prime to get the same pattern we need.

$$\sigma(2^{r)}) = \frac{2^{r+1} - 1}{2 - 1} = p$$

And

$$\sigma(p) = p + 1 = 2.2^r = 2^{r+1}$$

Notice that both these equations amount to the same thing, namely, $p = 2^{r+1} - 1$ it looks as if whenever we can find a prime that is one less than a power of 2 say $p = 2^k - 1$, Then $2^{k-1}p$ will be a perfect number, (here k is the $r + 1$ of the displayed equations This is true , but we well write out a formalproof just to make sure .

Theorem (2.13):

If k is any integer such that $2^k - 1$ is prime then $2^{k-1}(2^k - 1)$ is perfect

Proof:

Since $2^k - 1$ is an odd prime, it is relatively prime to 2^{k-1} thus by the multiplicatively of σ, we have

$$\sigma\left(2^{k-1}(2^k - 1)\right) = \sigma(2^k - 1)\sigma(2^k - 1).$$

Now byTheorem (2.4)

$$\sigma(2^{k-1}) = \frac{2^k - 1}{2 - 1} = 2^k - 1$$

While since $2^k - 1$ is prime $\sigma(2^{k-1}) = 2^{k-1} + 1 + 1 = 2^k$

We see that if $= 2^{k-1}(2^{k-1})$, then:

$$\sigma(n) = (2^k - 1) = 2^k = 2n$$

We now have a scheme for finding perfect numbers, being to construct one whenever we find a prime that is one less than a power of 2.

k	2^{k-1}	Prime	Perfect number
1	1	no	
2	3	yes	$2 \cdot 3 = 6$
3	7	yes	$2^2 \cdot 7 = 28$
4	15	no	
5	31	yes	$2^4 \cdot 31 = 496$
6	63	no	

The reader should check that 496 really is perfect, clearly the determination of when $2^k - 1$is a prime is an important question in the study of perfect a numbers. We defer this until the next section however, and turn instead to the equation of whether or not we are on the track of all perfect numbers.

That each primes of the form $2^k - 1$ guies a perfect appears in this Elements. This left the quations “Are there any perfect numbers not of Euclid’s form?” It took about 2000 years until progress was made on this questions and even than a complete answer was not given.

Theorem (2.14): (Euler):

Every even perfect number is of form $2^{k-1}(2^k - 1)$.

When $2^k - 1$is aprime?

Proof:

Suppose n is an even perfect number, Then we can write $n = 2^r q\ , r\ > 0$, where q is some odd integer. Using the multiplicatively of

$$\sigma(n) = \sigma(2^r)\sigma(q) = (2^{r+1} - 1)\sigma(q).$$

Note that we know nothing about q other then it is odd so we cannot evaluate $\sigma(q)$. From the fact that n is perfect.

However we have

$$\sigma(n) = 2.2^r.q = 2^{r+1}q$$

Combining. This with the previous equation and dividing through by $2^{r+1}\sigma(q)$giver.

$$\frac{2^{r+1}-1}{2^{r+1}}=\frac{q}{\sigma(q)}$$

This equation provides the key to the proof of thus theorem notice that the fraction on the left is close to 1, since the nominatoris only one less than the denominator, on the other hand, we would expect the fraction on the right to be smaller, since its denominator $\sigma(q)$ is asum including $q, 1$ and whatever other divisors q has no more divisors.

Of course, just because two fractions are equal does not mean that the same goes for their numerators and denominators the fractions might not be in lowest terms, since the numerator is odd , but it's not clear that the fraction on the right is, let us suppose $(q, \sigma(q)) \ = d$

They

$$q = d(2^{r+1} - 1) \ = \ d.2^{r+1} - d$$

And

$$\sigma(q) = d.2^{r+1} = q + d.$$

Now 2^{r+1}-1 > 1, so d is advisor of q other they q it self contradicts the last equation. We conclude that $d = 1$.

Setting $s = 1$ in the last equation gives $\sigma(q) = q + 1$.This clearly implies that q is prime the previous equation then says that $q = 2^{r+1}$-1 setting $k = r + 1$ setting $k = r + 1$ now yield that statement theorem.

Euler's theorem only covers perfect numbers, are there any odd ones, nobody knows, No one has ever found an odd perfect number, but neither has anyone ever shown that exist, and there might even be innately many of them in 1991 R-B Brent C.L. Cohen, and H.J.J to Ride published a paper showing that there is no odd perfect number less than 10^{300}.

Merseme and Fermat numbers:

In k is a positive integer we all the number $2^k - 1$ amersenne number and denote it by M_k.

Which mersenne numbers are prime?

Of course , we are interested in this questions because we have found that there is a are $-t$ -one correspondence between mersenne primes and even perfect numbers let us carry the table of the last section further .

k	$M_k = 2^k - 1$	Prime?
1	1	No
2*	3	Yes
3*	7	Yes
4	15=3.5	No
5*	31	Yes
6	63=9.7	No
7*	127	Yes
8	2.55=8.5.7	No
9	511=7.73	No
10	1023=3.11.31	No

The values of k making M_k prime have been starred in the table.

They are $k = 2{,}3{,}5$ and 7 – exactly the primes, the natural conjecture would be that M_k is prime exactly when k is prime. This is soon punctured, however, since $M_{11} = 2047 = 23.89$

In spite of this Christian wolf $(1679 - 1754)$ stated in print that 2,047 was prime . He even claimed that $M_9 = 511$ was prime 1)

Half of the conjecture is true. For M_k to be prime, k must be prime . In faction examination of our table seems to indicate that if d/k, then $M_d|M_k$. for example $, 2/4$, and $M_2 = 3/15 = M_4$ likewise . 26 and 3/6, and $M_2 = 3$ and $M_3 = 7$ both divide$63 = M_6$although there are many ways of proving that this works in general (see the problems at the end of the last section). By for the easiest is by means of congruence's.

Theorem(2.15):

Suppose $d\ and\ k$ are positive integers such that $d|k$ then $2^d - 1|2^k - 1$ thus if M_k is prime k must be prime .

Figure 2.1 A tune by Mersenne appear s in REdpighhi'sAncient Airs and Baances:

Proof:

we wish to show $2^k - 1 \equiv 0\ (mod\ 2^d - 1)$, or

$2^k \equiv 1\ (mod2^d - 1$, let $k = de$. Then since $2^d \equiv 1(mod2^d - 1)$ we have $2^k - 1 = 2^{de} - 1 = (2^d)^e - 1 \equiv 1^e - 1 = 0(mod2^d - 1)$

Where the congruence's follows from theorem.

1. Mersenne numbers the Mersnne numbers are of the form numbers. The mersnne numbers are of the form $2^n - 1$ as a result of the computation described below m it can now be stated that the first seventeen primes of this form correspond to the following values of

$$n = \ 2,3,5,7,13,17,19,31,61,89,107,127,521,607,1279,2208,2281.$$

The first seventeen even perfect numbers are therefore obtained by substituting these values of n in the expression $2^{n-1}(2^n - 1)$.

The first twelve of the mersenne primes have been know since 1914;

The twelfth,$2^{127} - 1$, was indeed found by Lucas as early as 1876. And for the next seventy-five years was the largest known prime.

Figure 2.2 Raphael Robinson tells about five new mersenne primes in the proceedings of the American Mathematical society 1954. He had never programmed a computer before of 2 that they get big quite fast, $M_{31}$is already more than two billion, The introduction of electronic computers has made it possible to check much larger numbers than before, As late as 1948 the largest k for which M_k was know to be prime was 127, which has been found by the French mathematician Lucas in 1876. It gave the prime.

$$M_{127} = 170, 141, 183, 460,469, 231, 687, 303, 715, 884, 105, 727.$$

Then computers turned up the temperatures. On January 30, 1952. During their infancy, Raphael M. Robinson applied a theoretical test originally devised by Lucas using. The SWAC (The national Bureau of standards, Western Automatic computer) computer in Los Anglos and found two new mersenne primes during the first day. He found three more that year, on June 2,5, October7, and October 9. (See figure 2.2) This brought to 17 the numbers of known mersnne primes, The SWAC computer took about eliminate to Jefer mine that the smallest of the new primes, $2^{521} - 1$ was indeed prime, and about an hour for the largest, $2^{2281} - 1$.

The total memory of the computer for both program and data was 256 words of 37 binary digits each and this restricted checking $2^h - 1$ for primness' to $n < 2304$.

In modern terns, the SWAC had about or memory much hoes than today's programmable calculators. These finds were surprised as computer got bigger and faster, The Post-age meter stamp shown in figure 3.3 was used by the university of I union is to honor the discovery of the prime M_{11213} there in 1963. In 1978 two 18-year-olds from Haney war 81 California – Laura Nickeland curt M_{21701}. The story in figure 3.4 appeared in the times if London.

Figure 3.3 university, if Illinois used postagemeter in 1983.

Hayward California, Nov.16.16-two 18-year-old American students have discovered with the help of a computer at California state university the biggest known prime number, two to the 21,701 power.

Laura Nickel and curt Noll received cognations from Dr. Bryant Tuckerman, an American who discovered the previous record holder among prime numbers : two to the 19,937th power- Agence France – pressed – Figure 3.4 two 18-year-olds found M_{21701}.

Now finding now mwersnne primes has become agroup activity. In 1996 George Wolman, an Orland, Florida programmer, started he great internet mersnne prime search (GTmps) by writing and distributing software that has enabled thousands of people to participate using their personal computers. The longest prime now known is $2^{6972593} - 1$, a number of 2,098, 960 digits. It was discovered June 30,199, by GTnps participant Nayem Hajrtwala, of Plymouth, Michigan. Hajiratwala, who works for price waterloos scoopers, used ei 350 MH_2 Pentium II IBM Actives computer part-time for 113 days to identify the prime.

In spite of the manymersnne primes that have been found no one has ever proved that there are infinitely many of them .

Summary of what is known and not known about prefect numbers.

1. If$2^k - 1$ is prime, then $2^{k-1}(2^k - 1)$ is a perfect number .

2. If n is an even perfect number, then it is of the from given in (z).
3. It is not known whether there are infinitely many even perfect number.
4. It is not known whether there are any odd perfect numbers at all.
5. If $2^k - 1$ is prime, then k is prime, but the converse is not true.

Fermat numbers:

Since the numbers $2^k - 1$ proved interesting we turn to the numbers$2^k + 1$.

k	$2^k + 1$	Prime?
1^*	3	yes
2^*	5	Yes
3	$9 = 3 \cdot 3$	no
4^*	17	Yes
5	$33 = 3 \cdot 11$	no
6	$65 = 5 \cdot 13$	no
7	$129 = 3 \cdot 43$	no
8^*	257	Yes
9	$513 = 3 \cdot 3 \cdot 3 \cdot 19$	no
10	$1025 = 5 \cdot 5 \cdot 41$	no

The values of k giving primes have again been starred in the table. So far, they are exactly the powers of 2: 1,2,4 and 8 . looking at the composite numbers in the second column we see the same divisor recurring, namely, 3 and 5, and these are themselves of the from $2^k + 1$.

If k is odd 3 sevens to divide $2^k + 1$, while if k is even (but not divisible by 4) 5 is divisor.

Our table suggests the conjecture that if $k = ab_1$ where a is off, then

$2^b + 1 | 2^k + 1$.

Although this may be proved direct division, congruence proof is much easier, and provides another demonstration of the usefulness of the congruence notation.

Theorem (2.16):

If k, a and b are positive integers such that $k = ab$ where a is odd, then $2^b + 1/2^k + 1$.. In particular, if $2^k + 1$ is prime, then k is 0 or a power of2 .

$proof$ .we wish to show $2^k + 1 = 0$ $(mod\ 2^b + 1)$, or$2^k \equiv -1$ $(mod 2^b + 1)$. Now $2^b \equiv -1 (mod 2^b + 1)$,

So

$$2^k = 2^{ab} = (2^b)^a \equiv (-1)^a \equiv 1 - (mod 2^b + 1)$$

where the first congruence follows from theorem 1,21 and the second from the fact that a is odd.

To prove the last sentence of the theorem we note that if k>0 is not a power of 2 then we can take a>1. Thus $1 < 2^b + 1 < 2^k + 1$, and so $2^k + 1$ has a positive division other than I and itself.

Definition (2.17):

Fermat numbers if r is nonnegative integer we $2^{2r} + 1$.

A Fermat number, and denote it byF_r.

Example (2.18):

$$F_0 = 2^{2^0} + 1 = 3, F_1 = 2^2 + 1 = 5,\ F_2 = 2^4 + 1 = 17$$

And

$$F_3 = 2^8 + 1 = 257$$

Fermat conjectured that they were. Since? Raised to a power of 2 involved, The Fermat numbers get large much faster than even the ,mersenne numbers and so it is much more difficult to tell whether they are prime of not. The number $F_4 = 65{,}537$ is not too big, and can be shown to be a prime but $F_5 = 2^{32} + 1$ is already greater than 4 billion. It took about 100 years after Fermat's conjecture for Euler to succeed in showing that F_5 was compositive. He used a theoretical method rather than merely checking the 10- digit number for factors. We will give a congruence proof that 641 divides F_5 involving very little arithmetic. First notice that $641 = 640 + 1 = 2^7 5 + 1$ and $641 = 625 + 16 = 5^4 + 2^4$ thus $2^7 5 \equiv -1(\text{mod } 641)$ and$2^4 \equiv -5^4(mod\ 641)$ Then (all congruence being module 641 and using theorem and $F_5 = 2^{32} + 1 = 2^{28} 2^4 + 1 \equiv (2^7)^4(-5)^4 + 1 \equiv -(-1)^4 + 1 = 0$.

We see Fermat's conjecture was incorrect. Worse than that, no other primes $F_r$have eis yet been found !many other values of rare known for which F_r is composite, but aside from these numerical results not much is known.

It is possible that F_r is also possible that other Fermat primes exist , even infinitely memy.

Just as mersenne primes apple to the study of perfect numbers, Fermat.

Primes arise in other parts of mathematics. They are connected with The construction of regular polygons in geometry. For example, the reason that irregular Pentagon can be constructed with straightedge and compass but irregular.

7- German mathematician guess proved that a regular polygon with $n > 2$sides is constructible if and only if n is a power of 2 times a product (possibly empty) of distance Fermat primes.

2.5 The Euler Phi Function measuringprimness'.

There has hardly been anything we have done up to now in which the prime number have not played an important role. Although being prime is an all or-nothing proposition, we have the feeling that some numbers any more composite them others.

For example $60 = 2 \cdot 2 \cdot 3 \cdot 5$ seems further from primness than $62 = 2 \cdot 31$ one way we might quantify this feeling is with $\tau(n)$, the number of positive divisors if n . Only if n is prime can $\tau(n)$ be 2, for composite number it is bigger.

In a certain since (the bigger $\tau(n)$ is the further n is from being prime. For example $\tau(62) = 4$, while $\tau(60) = 12$.

Another way to measure the same thing depends on the fact that if is prime, then $(p, n) > 1$ of and only of p/n. This property characterizes the prime, for if id composite , it has a divisor n such that icnca. Then $(a, n) > 1$but a dosen't divide n.

Other things being equal, we expect $(a, n) = 1$ to be a more common occurrence when a is composite.

As an example let us write out the first for n such that $(7, n) = 1$. The easiest way is to start writing out all the integers, crossing out the multiples of 7.

1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21

Let us now do the something with 6 instead of 7. Since $(6, n) > 1$ if and only id some prime divides both n and only if some prime divides both n and $6 = 2.3$, it suffices to cross multiples of 2 and 3.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18

Then n such that $(6, n) = 1$ appear to be much rare. The reader has probably noticed a pattern in the two arrays just presented. Wither all or none of the numbers in each column have been crossed out, This is no surprise if we recall that theorem says that if $b \equiv b' \ (mod\ a\ )$, then $(a, b\ ) = (a, b')$. In particular $((a, b) = 1$ if and only if $((a, b') = 1$.

In the first array we listed the numbers in 7 columns consisted of numbers congruent module 7. In the second array, The columns consisted of numbers congruent Module 6. By the argument in the previous paragraph, either all the numbers in a given column are relation prime to $a\ (= 6\ or\ 7)$, or else none are.

Since we cannot count all the n such that $(a, n) = 1$, There being infinityely many of then let us merely count those in the "first row: after that the pattern repeats anyway.

Definition (2.19):

Euler $\emptyset$ function suppose a is a positive integer. we define $\emptyset(a)$ to be number of integers $n, 1 < n < a$ that $(a, n) = 1$.

The function $\emptyset$ is called the Euler phi function.

Example (2.20):

By what we have already seen, $\emptyset\ (6)\ = 2\ end\ \emptyset\ (7)\ = 6$.

Clearly $\emptyset(p)\ = p - 1$ for any prime p.By definition.$\emptyset\ (1) = 1$.

Let us compute $\emptyset(12)$since $12 = 2^2 3$, it suffices to cross out the multiples of 2 ane 3 from among the first 12 integers : 1 2 3 4 5 6 7 8 9 10 11 12 we see $\emptyset(12)\ = 4$.

A short out to computing $\emptyset(\boldsymbol{n})$

Computing $\emptyset(12)$ by our crossing method amounted to eliminating the same numbers as in computing $\emptyset(6)$ the multiplied of 2 and 3. Thus the numbers left are exactly the same as in the first two rows of our table for 6 above , and the pattern from 7 to 12 repeats that of through 6. If we had noticed this at the start we could have cut our work in half. we could have crossed out the multiples if 2 and 3 among the first integers leaving 2 numbers, then doubled this count of 2 to get $\emptyset(12) = 4$. In other words, $\emptyset(12) = 2\,\emptyset(6)$ .In the same way, $\emptyset(18) = 3\emptyset(6) = 6, \emptyset(30) = 8 \neq 5\emptyset(6)$.

Proposition (2.21):

If k and a are positive integers such that all primes dividing k also divide a , then $\emptyset(k\,a\,) = k\emptyset(a)$.

Proof consider the array,

$$\begin{array}{ccc} 1 & 2 & a \\ a+1 & a+2 & \cdots\ 2a \\ (k-1)a+1 & (k-1)a+2 & \ldots.ka \end{array}$$

Let us cross out the entries that are not relatively prime to key in order to compute $\emptyset(ka)$. This amounts to crossing out everything not relatively prime to a since $(a,n) > 1$ if and only if some prime divides both a and n, and the same primes divided ka divide a by Theorem(1.20) the pattern of crossing out is the same in each row. Since there are $\emptyset(a)$ entries left in all. Thus $\emptyset(ka) - k.\emptyset(a)$.

Example (2.22):

Since 3 is prime, $\emptyset(3) = 3 - 1 = 2$. Thus

$$\emptyset(27) = \emptyset(9.3) = 9 \cdot \emptyset(3) = 9 \cdot 2 = 18.$$

We can apply proposition G because 3 is the only prime dividing.

Proposition G goes along toward a formula for $\emptyset(n)$. For example, suppose we want to compute$\emptyset(1{,}000{,}000)$.We have

$$\emptyset(10^6) = \emptyset(2^6 5^6) = \emptyset(2^5.5^5.2.5) = 2^5.5^5.\emptyset(10),$$

but$e$ still must compute $\emptyset(10)$ by actual. The computation of $\emptyset(n)$ can always be reduced in the some way to that of a product of distance primes if we could pull the p_1 out of $\emptyset(p_1p_2 \ldots \ldots p_t)$ just as we learned to pull the k out of $\emptyset(ka)$under the hypothesis of proposition G we could write a complete formula. Let us see if we can modify the proof of proposition G to compute ∅(pa), where P is a prime not dividing a. As before , let us write out The integers from L to Pa.

$$\begin{matrix} 1 & 2 & & a \\ a+1 & a+2 & \cdots & 2a \end{matrix}$$

$$(p-1)a+1 \ (p-1)a+2 \ldots .pa$$

Again let us imagine crossing out the n such that $(Pa, n) > 1$. The difference here is that $(Pa, n) > 1$is not equivalent to (a, n) >1 the latter implies the form the farm or but not conversely. Thus of the $P. \emptyset(a)$ integers left after crossing out all n such that $(a, n) > 1$ more still must be delimited, namely, the multiples of P. These are just $IP, 2P \ldots ap$. Of these those Kp such that $(k,\ a) > 1$ have already been eliminated and there are just $\emptyset(a)$ more to cross out in order that $\emptyset(pa)$ be property counted. Thus $\emptyset\ (Pa) = P\,\emptyset(a) - \emptyset(a) = (p-1)\,\emptyset(a)$ we have proved the following theorem.

Proposition (2.23):

If a is a positive integer, P is prime and P doesn't divide a then $\emptyset(Pa) = (p-1)\,\emptyset(a)$.

Example (2.24):

$$\emptyset(10^6) = 10^5\emptyset(2.5) = 10^5(2-1)\emptyset(5) = 40{,}000$$

$$\emptyset(60) = \emptyset(2^2.3.5) = 2.\emptyset(2.3.5) = 2(2-1)\emptyset(3.5) = 2(3-1)\emptyset(5) = 16$$

$$\emptyset(62) = \emptyset(2-31) = (2-1)\emptyset(31) = 30.$$

Theorem (2.25) :

If $n = p_1^{k_1}p_2^{k_2} \ldots \ldots \ldots \ldots .. p_t^{k_t}$ where $p_1p_2 \ldots \ldots \ldots \ldots, p_t$ are doesn't primes and $k_1, k_{21}, \ldots \ldots \ldots, kt$ are positive integer : Then

$$\emptyset(n) = \prod_{i=1}^{t} (p_i - 1)p_i^{k_i - 1}$$

Proof;

let $Q = p_2^{k_2} p_3^{k_3} \dots \dots \dots . . p_t^{k_t}$ then using propositions G and H we have $\emptyset(\mathrm{n})$ $= \emptyset(\mathrm{p}_1^{\mathrm{k}_1}\mathrm{Q}) = \mathrm{p}_1^{\mathrm{k}_1 - 1}\ \emptyset\ (p_1 Q) = \mathrm{p}_1^{\mathrm{k}_1 - 1}(p_1 - 1)\emptyset(\mathrm{Q})$.

The same technique may be applied to the prime powers in Q until we arrive at the formula if the theorem.

Example (2.26):

$$\emptyset(60) = \emptyset(2^2 . 3.5)(2 - 1)2(3 - 1)(5 - 1) = 16$$

$$\emptyset(62) = \emptyset(2.31) = (2 - 1)(31 - 1) = 30$$

$$\emptyset(360) = \emptyset(2^3 . 3^2 5) = (2 - 1)2^3(3 - 1)3(5 - 1) = 96$$

It not hard proves that $\emptyset$ is multiplicative now we have a formula for it, in fact, we leave this proof for the exercise. note that this reverses our practice of late of first proving a function multiplicative and then using this fact to derive a formula.

Theorem (2.27):

The function $\emptyset$ is multiplicative. Now consider the function F defined by

$$F(n) \sum_{d/n} \emptyset(\mathrm{d}).$$

Not that if P is Prime and k is a positive integer, then

$$f(p^k) = \sum_{d/n} \emptyset(\mathrm{n})$$

Not that if P is prime and K is a positive integer, then

$$F(p^k) = \sum_{d/p^k} \emptyset(p^k) = \emptyset(1) + \emptyset(P) + \dots . . + \emptyset(p^k)$$

$$= 1 + (p - 1) + (p - 1)p + \cdots + (p - 1)p^{k-1}$$

$$= 1 + (p - 1)(1 + p + p^2 + \cdots p^{k-1})$$

$$= 1 + (p - 1)\sigma(p^{k-1})$$

$$= 1 + (p - 1)\frac{p^k - 1}{p - 1} = p^k$$

since$F$ is multiplication by the previous theorem we have proved the following result.

Theorem (2.28):

If n is any positive integer or them

$$\sum_{d/n} \emptyset(d) = n$$

The möbius Inversion formula:

In section we saw that finding a formula for a numericalfunction was easier if w knew that it was multiplicative for in that case we had only to determine its value a prime powers. Theorem states that if two numerical functions fem F are related by

$$F(n) = \sum_{d/n} f(d), n = 1,2, \dots \dots ....$$

Then F is multiplicative whenever $F$is. If is a simple function, then it may be. Easy to show it multiplicative from which the multiplicativeof F follows.

Example are

$$F(n) \ = 1, f(n) = \tau(n) \ and \ f(n) = n, f(n) = \sigma(n).$$

Given numerical function f can we always finds a function f so that holy's? We will answer this question below.

Let us start with assessable an example as we can consider the function

$$f(n) = 1, n = 1,2, \dots \dots ..$$

We will try to find of function f such that holds.

Taking $an = 1$ in we get $F(1) = f(1)$, and so $f(1) \ = F(1)$, taking $n = 2$ yields $F(2) = f(2) + f(1)$. or $1 = f(2) + 1$,and so we must have $f(2) = 0$ Likewise using $n = 3$ we get $F(3) = f(1) + f(3)$, or $1 = 1 \ + f(3)$, and so $f(3) \ = 0$ also. In the same way$F(4) = f(1) + f(2) + f(4)$ or $1 = 1 + 0 + f(4)$ implying that $f(4) \ = 0$.

If appears that we way have $f(1) = 1$ and $f(n) = 0$ for $n > 1$. Let us not lose sight of our calculate ions show that if such a function f exist. Then of necessity$f(1) = 1$, and $f(2) = f(3) = f(4) = 0$.

Such computations do not establish the existence of such a function, however. An analogs situation.

CHAPTER THREE
THE ALGEBRA OF CONGRUENCE CLASSES

Solving linear congruence:

What does it mean to solve congruence?

The reader knows what it means to solve the equation $x^2 + x - 2 = 0$

For example, we must find all values of x making the equation true; we will consider the similar problem where the equality sign is replaced by " $\equiv$ ". In general, we will restrict ourselves to congruence of the form

$$f(x) \equiv 0 \ (mod\ b).$$

Where$f(x)$ is a polynomial in $x$with integer coefficient supposed ?$x_1\ e$.

Satisfies the congruence

$$x^2 + x - 2 \equiv 0 \ (mod\ 7)$$

and suppose that $x_2 \equiv x_1(\text{mod}7)$. Then by Theorem (1.5)

$$x_2^2 + x_2 - 2 \equiv x_1^2 + x_1 - 2 \equiv 0(mod\ 7),$$

and so x_2 is also a solution of the congruence, thus if we find one solution $x_1$we immediately have infinitely many more solution s, namely, all integers congruent to x modulo 7 since we cannot write all of these down, we will content ourselves with identifying any one of them, and the one we identify will serve since Theorem applies to any polynomial with integer coefficients, we have following general result.

Theorem (3.1):

Let x_1, x_2 and $b > 0$ be integers, with $x_1 \equiv x_2(mod\ b)$, and let f be a polynomial withinteger coefficients, then x_1 is a solution to

$f(x) \equiv 0(mod\ b)$if and only ifx_2 is. It's convenient at this point to introduce names for various sets of integers of importance for a given modules.

Complete reticule system suppose $b >\ 0$ by a congruence class module b. We mean the set of all integers congruent module to some fixed integers such that exactly one integer in the set in each congruence class module b.

Example (3.2):

There are three congruence classes module 6 $= 3$, namely

$$\{\dots\dots\dots, -6, -3\ ,0\ ,3\ ,6, 9, \dots\dots\dots\}$$

$$\{\dots\dots\dots.,,05,02,1, 4, 7, 10\ , \dots\dots\dots\}$$

and

$$\{\dots\dots\dots, -4\ , -1\ ,2\ ,5\ ,8, 11, \dots\dots\}$$

One complete residue system modulo 3 is {0,1,2}.

Another is $\{1, 2, 3\}$ another is $\{\ 10\ , -1\ , 6\}$.

If we write out the integers in atable with rows of length b, as has proved useful several times, then the columns are exactly the congruec classes modulo b, taking $b\ = 4$, for example . We get

.	.	.	.
.	-6	-5	-4
-3	-2	-1	0
1	2	3	4
5	6	7	8
9	10	11	.
.	.	.	.,

and each column is a congruence class modulo 4 If we chose exactly one number from each column, say $5, -2\ , 11$ and 0, we get a complete residue system modulo 4. It is easy to see that there are exactly to congruence classes modulo b, and that any complete residue system modulo b also consists of exactly b elements.

Recall that if F is a polynomial with integral coefficients then any integer congruent modulo 6 to a solution to

$$f\ (x) \equiv 0\ (mod\ b)$$

is also automatically a solution, and so doesn't deserve separate attention . This is the reason for the following definition.

Definition (3.3):

Complete solution, least complete solution we call $x_1, x_2, \dots\dots., x_k$ a complete solution to the congruence (3.1) in case it is the set of all solutions in some complete residue system modulo 6. It is the least complete solution in case it is the set all solution among $0,1, \ldots\ldots, b-1$.

Example (3.4) :

Consider the congruence

$$4x - 18 \equiv 0 \ (mod\ 6)$$

Among the integers 1,2,3,4,5,6 exactly 3 and 6 satisfy the congruence, thus x=3,6 is a complete solution. Another complete solution is $x = -3,0$,since , these are all solution in the complete residue system $-3,-2,-1\,,0\,,1\,,2$, Another is $x = 0,3$..

Note that it is possible to match up the elements of any the complete solutions so that corresponding numbers are congruent modulo 6 for example,

$$9 \equiv 3 \ and \ 72 \ \equiv 6 \ (mod\ 6)$$

one the other land, $x = -3,9$, is not complete solution to $x - 18 \equiv 0 \ (\,mod\ 6\,)$ since -3 and 9 are in the same congruence class.

In this chapter we will consider only congruencies $f(x) \equiv 0(mod\ b)$; where f is a liner polynomial. Such a congruence can be put in the form $ax \equiv c\ (mod\ b)$, to solve this congruence we must look for values of x such that $b/6 - axi$ that is, such that case by for some integer y, this is the equation $ax + by = c$ that we analyzed completely in section (3.1) there we decided that:

i- The equation $ax + by = x$ has a solution if and only if (a,b) divides c.

ii- Asolutioncan be found example by using the Euclidean, algorithm to find (a,b) and then solving the equations background.

iii- If x_0, y_0 is a particular solution then all solutions are given by

$$x = x_0 + \frac{bt}{d}, y = y_0 - at/d$$

Where turns through.

iv- The integers and $d = (a,b)$

We will illustrate the is of (i) and (ii) to find a solution to

$$147x \ \equiv 77\ (mod\ 161)\,.$$

Here $a \;=\; 147, b \;= 161$ and $c = 77$. First we sue the Euclidean algorithm find $(147, 161)$.

$$161 \;=\; 1 \cdot 147 + 14$$
$$147 \;=\; 10 \cdot 14 + 7$$
$$14 \;=\; 2 \cdot 7 + 0$$

We see that $(147{,}161) \;=\; 7$ and since 7 divides 77,

The congruence has a solution now we solve the equations backward as follows:

$$7 = \;147 - \;10 \cdot 14$$
$$= \;147 - 10(161 - 147)$$
$$= 11 \cdot 147 - \;10 \cdot 161$$

Multiplying through by $77\;/7 \;=\; 11$ gives

$$77 \;=\; 121.147 - 110\,.161$$

We have found one solution to the congruence, namely , $x \;= 121$ now let us see how (iii) tells us how to find a complete we know that if x_0 is one solution to the corresponding equation then all solutions are given by $x = x_0 + \frac{bt}{d}$, where $d = \;(a, b)$ and t runs through the integers . This gives infinitelymany values of x, but we only want to find the solution s in some complete residue system modulo b; that is , we want at most one solution in any congruence class modulo b .

How is it possible for us to have .

$$x_0 + \frac{bt}{d} \equiv x_0 + \frac{bt'}{d}\;(mod\;b)$$

For integers $t$and t? This amounts to the fact that b divides

$$x_0 + \frac{bt'}{d} - \left(x_0 + \frac{bt}{d}\right) = \frac{(t'-t)b}{d}.$$

They

$$(\grave{t}\; - t)b/d \;= kb.$$

Or $\acute{t}\; - t \;=\; kd$ for some integer k, that is $\grave{t}\;\equiv t\;(mod\;d)$.

Thus using only values of t in congruent modulo b. Furthermore, we will not miss any solution x in congruent modulo b. Furthermore, we will not miss any solutions this way, for it can be shown that $t^1 \equiv t\ (mod\ d)$ implies that:

$$x_0 + \frac{bt}{d} \equiv x_0 + \frac{b\grave{t}}{d}(mod\ b);$$

See the exercises at the end of this section, we see that if the values s of t are restricted to the in some complete residue system modulo $d = (a, b)$, then the values of $x = x_0 + \frac{bt}{d}$ will be in congruent modulo b m and will comprise a comprise a complete solution,

Theorem (3.5):

Consider the congruence $ax \equiv c\ (mod\ 6)$ this has a solution if and only if (a, b) divides c, if x_0 is any solution if and only if solution is given by the numbers:

$x = x_0 + \frac{bt}{a,b}$where$t$ runs through any compete residue system modulo (a, b) .

Example (3.6):

We return to the congruence $147x = 77\ (mod\ 161)$. For which we have already found a particular solution x = 121. We also found that congruence is given by :

$$x = 121 + \frac{161t}{7} = 121 + 23t$$

Where t runs through any complete residue system modulo7 letting $t =$ 0,1,2,3,4,5,6, yields the complete solution

$$x = 121,144,167,190,213,236,259,$$

(note that taking $t\ = 7$ gives $x\ =\ 282$, but $282\ \equiv 121\ (mod\ 161)$ the least complete solution is

$$x = 121, 144,167 - 161 = 6, 190 - 161 = 29, 213 - 161 = 52, 236 - 161 \\ = 75,259 - 161 = 98.$$

Example (3.7):

Solution $15x \equiv 50\ (mod\ 100)$ inspection we find the particular solution $x_0 = 10$ we also note that $(15{,}100)\ - 5$, than a complete solution is given by:

$$x = 10 + \frac{100t}{5} = 10 + 20t$$

Where $t\ = 0{,}1{,}2{,}3{,}4$ we get $x\ = 10{,}30{,}50{,}70{,}90$ as a complete solution (it is also least complete solution)

Example (3.8):

Find a complete solution to the congruence 148 $x \equiv 999\ (mod\ 2222)$.

Here

$$2222 = 1.1485 + 737$$

$$1485 = 2, 14737\ +\ 11$$

$$737\ =\ 67\ .11\, so\ \ (1485, 2222) = 11$$

But 11 doesn't divide 999 and 30 there are no solutions,

Example (3.9):

Find a complete solution to $45x\ \equiv 3\ (mod\ 48)\ = 3$, a complete solution is

$$x =\ -1\ +\ \frac{48t}{3} = -1 + 16t;$$

where$t = 0, 1, 2$ this gives $x =\ -1, 15\ , 31.$

Now -1 and 15 are the elements smallest in absolute value in their congruence classes, but ti fulfill the conditions of the, problem we must replace 31 by $31 - 48\ =\ -17$. Thus the answer is $x\ =\ 17\ , -1\ , 15.$

The Chinese Remainder Theorem:

Simultaneous congruence's:

Suppose a and t are relatively prime positive integers, by Theorem (3.6) we can chose x so that ax is in any congruence .class we want modulo b . For that matter we can also chose y so that by in any congruence class we want modulo $a.$ to emphasize the symmetry between a and b we will change the notation and consider relatively prime positive integers b, and $b_1$and b_2 by theorem (3.6) we can find x_1 such that ,

$b_2x_1 \equiv 1\ (mod\ b_1)$ then :

$$b_2x_1c_1 \equiv c_1(mod\ b_1);$$

Where c_1 is completely arbitrary. Likewise we can find $x_2$such that $b_1x_2 = 1(mod\ b_2)$, where c_2 is arbitrary.

The important implication of the above congruence's is that we can make the sum $z = b_2x_1c_1 + b_1x_2c_2$ simultaneously congruent to whatever we want modulo both b_1 and $b_2\ for$

$$z = b_2x_2c_1 + b_1x_2c_2 \equiv b_2x_1c_1 + 0 \equiv c_1(mod\ b_1)$$

And

$$z = b_2x_1c_1 + b_1x_2c_2 \equiv 0 + b_1x_2c_{2=}\, c_2(mod\ b_2)$$

the ability to find an integer 7 such that

$$z = c_1(mod\ b_1)\text{and } z = c_1(mod\ b_1)$$

Where c_1 and c_2 are arbitrary, has many applications.

Example (3.10):

Professor snabley feeds his pet python every four days and bathes it once a week. This week he fed it on Tuesday and washed it on Wednesday, when, if ever, will he fed and wash the python on the same day? How often will this happen?

Let us number the days, with Tuesdayas day 1, then the snake will be fed on days $1, 5\ ,9\ \ldots\ldots$, and, in general, on day z exactly when $z \equiv 1\ (mod\ 4)$.

Since he washes the snake every seven days beginning with Wednesdays (day 2), day z is a washday exactly when $z \equiv 2\ (mod\ 7)$. Because the module 4 and 7 are relatively prime, the simultaneous congruence's.

$$z \equiv 1\ (mod\ 4)\ \ and\ z \equiv 2\ (mod\ 7)\ (3.2)$$

Will have a solution by the proceeding analysis, let us take $b_1 = 4, c_1 = 1, b_2 = 7,$, and $c_2 = 2,$ we start by finding an integer x_1 such that $b_2x_1 \equiv 1\ (mod\ b_1)$or $7x_1 \equiv 1\ (mod\ 4)$. One solution is $x_1 = 3,$ likewise we want x_2 such that $b_1x_2 \equiv (mod\ b_2$or $4x_2$ ≡1 (mod 7) A solution is $x_2 = 2.$ Now according the computations at the beginning of this section a solution to (3.2) is

Is

$$z = b_2x_1c_1 + b_1x_2c_1 = 7\cdot3\cdot1\ +\ 4\cdot2.2\ =\ 37$$

we easily check that indeed .

$$37\ \equiv 1\ (mod\ 4) \text{ and } 37\ \equiv 2\ (mod\ 7).$$

Thus the snake will be washed and fed on day 37.

How often the snake gets washed and fed on the same day is another question. By (3.2) it happens on day 7 exactly when

$$z\ \equiv 1\ \equiv 37\ (mod\ 4) \text{ and } 7 \equiv 2 \equiv 37\ (mod\ 7).$$

This means $4/37 - z$ and $7/37\ - z$, which is clearly equivalent to $4\cdot7\ =\ 28//37 - z$. Thus the snake will be the end eat when z ≡37 (mod 28), every 28 days. The next time this will happen will be on day $9 = 37 - 28$, which is Wednesdays of next week.

The congruence property of 4 and 7 mentioned at the end last example works for any relatively prime positive integers, the proof of the following theorem is left for the exercises.

Theorem (3.11):

Let b_1 and b_2 relatively prime positive integers, and let z and $\grave{z}$be any integers, then $z = \grave{z}(mod\ b_1)$

If and only if $z\ \equiv \grave{z}(mod\ b_1b_2\ )$

Now let us try to solve $z \equiv \begin{cases} c_1(modb_1) \\ c_2(modb_2) \\ c_3(modb_3) \end{cases}$

Where(b$_{1,}$b$_2$) = (b$_{1,}$b$_3$) = (b$_{2,}$b$_3$) = 1, It seems natural to expect 7 to be sum oftheir terms two which are congruent to 0 modulo bi for any particular I consider .

$$z = b_2b_3x_1c_1 + b_2b_3x_2c_2 + b_1b_2x_{31}c_3$$

Note that whatever x_1, x_2 and x_3 are

$$z = b_2b_3x_1c_1 + 0 + 0 \equiv b_2b_3x_1c_1\ (mod\ b_1)$$

Note since b_1 is relatively prime to b_2 and b_3 , we have $(\ b_1b_2b_3) = 1$ bycorollary(1.12) thus we can chose x_1 so that

$b_2b_3x_1 \equiv 1\ (mod\ b_1)$, and80$b_2b_3x_1c_1 \equiv c_1\ (mod\ b_1)$

A similar argument works for the modulo $b_2$and b_3. Let us make things look simpler by introducing now notation,

Let $B\ =\ b_1b_2b_3$, and set $B_1 = b_2b_3 = B/b_1, B_2 = B/b\ _2$and $B_3 = B/b_3$. Then our solution to is $z = B_1x_1c_1 + B_2x_2c_2 +\ B_3x_3c_3$, where x_i satisfiess $B_ix_i \equiv 1\ (mod\ b_i)$ for $i = 1,2,3$.

Example (3.12):

Consider the system

$$z \equiv 2\ (mod\ 3)$$
$$z \equiv 5\ (mod\ 4)$$
$$z \equiv 3(mod\ 7)$$

This is solvable, since (3,4) = (3,7) = (4,7) = 1 we have $b_{1=}3, b_{2=}4,\ b_{3=}7$ and , $c_{1=}2, c_{2=}5, c_{3=} - 3$,

so

$$B = 3.4.7\ =\ 84, B_1 = \frac{84}{3} = 28, B_2 = 21, and\ B_3 = 12,$$

the congruence $\quad 28x_1 \equiv x_1 \equiv 1\ (mod\ 3)$

$$21x_2 \equiv x_2 \equiv 1\ (mod\ 4)$$
$$12x_3 \equiv 5x_3 \equiv 1\ (mod\ 7)$$

Have the solutions x_1=1, $x_2 = 1$ and $x_2 = 1$ and $x_3 = 3$ thus a solution to the original system is

$$z = B_1x_1c_1 + B_2x_2c_{2+}B_3x_3c_3$$
$$= 28.1.2 + 21.1.5 + 12.3.(-3) =\ 53$$

Definition (3.13):

Relatively prime in pairs:

We say the integers $b_1b_2, \ldots\ldots b_n$ are relatively prime in pairs incase $(b_ib_j) =$ 1whenever $i \neq j$ for Example 3.4 and 7 are relatively prime in pairs, but s,4, and 6 are not , even though no integer greater than 1 divides all.

The following theorem extends the last result to n congruences it gets its name from the fact that it was introduced into European mathematics from chine's writings, It was known to the Chinese at least as early as the first century A.D we leave the proof for the exercise at the end of this section.

Theorem (3.14):

The Chinese reminder theorem)

Let $b_1, b_2, \ldots\ldots, b_n$ be integers greater then 0, relatively prime in pairs, and let $c_1, c_2, \ldots\ldots, c_n,$ be any integers, consider the system of congruence's .

$$z \equiv c_1(mod\ b_1)$$
$$z \equiv c_2(mod\ b_2)$$
$$.$$
$$.$$
$$.$$
$$z \equiv c_n(mod\ b_n)$$

Let B=$b_1 b_2 \ldots\ldots\ldots\ldots b_n$ and $b_i = B/b_i$for $i = 1,2,, \ldots\ldots\ldots, n,$ Let $x_i$be a solution to $B_i x_i \equiv 1\ (mod\ b_i)$

For $i = 1,2, \ldots\ldots\ldots, n,$ then a solution to the original system of congruences

$$z = \sum_{i-1}^{n} B_i x_i c_i$$

Furthermore $\acute{z}$ is another solution and only if $\acute{z} \equiv\ z\ (mod\ B)$.

Example (3.16) :-

Find all solutions $z, 0\ < z <\ 500$, to

$$z\ \equiv\ 1\ (mod\ 2)$$

$$z\ \equiv\ 2\ (mod\ 3)$$

$$z\ \equiv\ 3\ (mod\ 5)$$

$$z\ \equiv\ 4\ (mod\ 7)$$

We take b_1 =2, $b_2 = 3, b_3 = 5, b_3 = 7$,$c_1 = 1$,$c_2 = 2$,$c_3 = 3$, $c_4 = 4$

$B = 210, B_1 = 105$, $B_2 = 70$, $B_3 = 42$, and $B_4 = 30$ we must solve the congruence

$$105\ x_1 \equiv 1\ (mod\ 2)$$

$$70\ x_2\ \ \equiv 1\ (mod\ 3)$$

$$42\,x_3 \quad \equiv 1\ (mod\ 5)$$
$$30\,x_4 \quad \equiv 1\ (mod\ 7)$$

We can take $x_1 = 1, x_2 = 1,\ x_3 = 3,\ x_4 = 4,$ thus a solution is$z =\ 105, 1 \cdot 1 + 70\ \cdot 1 \cdot 2\ +\ 42 \cdot 3 \cdot 3\ +\ 30 \cdot 4 \cdot 4\ =\ 1103$ Since$B\ =\ 210$ all solutions are if the form $1103\ +\ 210\,t$. Solving$0\ <\ 1103\ +\ 210\,t\ < 500$ leads to

$$-5\frac{53}{210} < t\ < -2\frac{183}{210};$$

And $t\ =\ -5, -4\ , -3$. The corresponding solutions are $z =\ 53{,}263$and 473.

Reduced Residue system:

Now we return to the consideration of fixed modulus b. A complete residue system contains exactly one element in each congruence class modulo b, but sometimes we are only interested integers relatively prime to b.

Definition (3.15):

Reduced residue system:

By a reduced residue system modulo b we mean all integers relatively prime to b in some complete residue system modulo b.

Example (3.16):

Since 1,2,3 4,5,6 is a complete residue system modulo 6, a reduced residue system modulo 6 consists of 1 and 5, other are $\{7{,}5\}, \{\ -1{,}1\}$and $\{61{,}65\}$ .One reduced residue system modulo 5 is $\{1{,}2{,}3{,}4\}$ another is $\{(1{,}12{,}23{,}34)\}$.

Note that any two reduced residue systems modulo b have the same number of elements, namely, the number of congruence classes of integers in the complete residue system $1{,}2, \dots\dots, b$ relatively prime to be is by definition $ø\ (b)$:

Any reduced residue system modulo to have$ø\ (b)$ elements.

Theorem (3.17):

If a and $b\ > 0$ are relatively prime integers, then as x runs through a complete or reduced residue system modulo b, so does ax.

Proof:

As x runs through a complete residue system modulo b the integers ax are distinct modulo b by the cancellation theorem.

Since there are b of them, they also form a complete residue system modulo.

Likewise as x runs through a reduced residue system modulo b.

The integers ax are distinct modulo b by the same argument, they also form a reduced residue system modulo.b

Example (3.18):

A complete residue system modulo $b = 8$ is $\{-2,-1,0,1,2,3,4,5\}$ and a reduced residue system is $\{-1,1,3,5\}$. we take $a = 3$

The reader should check that $\{-6,-3,0,3,6,9,12,15\}$ is also a complete residue system $(mod\ 8)$, and that $\{-3,3,9,15\}$ is a residue system $(mod\ 8)$.

The theorems of Fermat and Euler:

How powers fall into congruence classes. assume a and b are relatively prime. Let us examine the powers of $a(mod\ b)$. Taking $a\ =\ 2$and $b = 7$, for example we have,

n	1	2	3	4	5	6	7
a^n	2	4	$8 \equiv 1$	$16 \equiv 2$	$32 \equiv 4$	$64 \equiv 1$	$128 \equiv 2$

Here all the congruences are modulo 7 . we have done more work in the above table than we needed to, since, for instance, once we complete the table up to $2^3 \equiv 1$, we have $2^4 \equiv 2^3 \cdot 2\ \equiv 1 \cdot 2\ \ \equiv 2, 2^5 \equiv 2^3 \cdot 2^2 \equiv 4$, etc

Clearly the pattern of least residues 2,4,1,2,4,1, … …will repeat forever . In the general case, since there are only finitely many congruence classes modulo b,eventually two powers of a will have to fall into the same class, But if $a^i \equiv a^j\ (mod\ b)$; then $a^{i+1} \equiv a^{j+1}\ (mod\ b)$follows from multiplication by a; And the pattern repeated, let us look at this process more closely. Suppose holds with i<j this can be written $a^i.1 \equiv a^i\, a^{j-i}(\text{mod b})$. Now $(a^i, \text{b}) = 1$,and so by the cancellation theorem $a^{j-i} \equiv 1\ (mod\ b)$.

We see that some power of a must be congruent to 1 modulo n.

Definition (3.19) The order of $\boldsymbol{a}$modulo $\boldsymbol{b}$:

Let a and$b\ > 0$ be relatively prime integers. By the order of a modulo b we mean the least positive integer k such that $a^k \equiv 1\ (mod\ b)$.

Example (3.20):-

Form our previous calculation the order of $2\ (mod\ 7)$is 3 the following table shows the successive powers $a^n$of $a\ =\ 1{,}2{,}3{,}4{,}5{,}6\ (mod\ 7)$ until we hit 1

	n	1	2	3	4	5	6	order
a								
1		1						1
2		2	4	1				3
3		3	2	6	4	5	1	6
4		4	2	1				3
5		5	4	6	2	3	1	6
6		6	1					2

In the table powers have been replaced by congruence elements of the reduced residue system 1,2,3,4,5,6 for example

$$3^2 = 9 \equiv 2\ (mod\ 7).$$

Suppose a has the order k (mod b) . Then if m is any multiple of k, say $m\ =\ kt$, we have

$$a^m = (a^k)^t \equiv 1^t\ \equiv 1(mod\ b).$$

Conversely, $a^n = 1\ (mod\ b)$, use the division algorithm to writte $n\ = kq + r, 0 = \leq r\ < k$. then

$$a^n = a^{kq+r} = (a^k)^q\ a^r \equiv a^r \equiv 1\ (mod\ b).$$

But this contradicts the assumption that k is the smallest positive integer such that $a^k \equiv 1\ (mod\ b)$ unless $r = 0$, thus we see that k/n. We have already seen that if $a^i \equiv a^j (mod\ b)$with $\ i <\ j$. Then $a^{j-i} \equiv 1\ (mod\ b)$,

And $k \backslash j - I$. In particular, no two powers of a up to the kth power can be congruent modulo.b We sum up what we have proved in the following theorem.

Theorem (3.21):

Suppose a and $b\ >\ 0$ re relatively prime integers, and let k be the order of $a$modulo b. then the numbers $a^1, a^2, a^3, \dots\dots\dots.\, a^k$ are in congruent modulo b and every positive power of a is congruent to one of them. Furthermore of m is a positive integer than

$$a^m \equiv 1\ (mod\ b) if\ and\ only\ if\ k/m.$$

We found that the six elements of a reduced residue system modulo 7 had orders as follows:

Element	1	2	3	4	5	6
Order	1	3	6	3	6	2

Notice that the orders 1,2,3 and 6 , are all divisors of 6 $= ø(7)$

If we take $b = 15$, then a reduced residue system has$ø(15) = 8$ elements . The reader should confirm that he following table gives the correct orders of these elements

Element	1	2	4	7	8	11	13	14
Order	1	4	2	4	4	2	4	2

Here the order are 1,2and 4, all divisor of 8. In each case every order is a divisor of $ø(b)$ it appears that it may be true that the order of any element a modulo b is always advisor of $ø(b)$. In light of the least. Theorem, the is equivalent to saying that $a^{\emptyset(b)} \equiv 1\ (mod\ b)$ .Whenever $(a, b) = 1$.

In order to prove this is it seems natural to try to associate the number a with a reduce residue system modulo b in some way.

Since the latter has exactly $ø(b)$ elements. Theorem (3.19) suggests multiplication;if $x_1, x_2, \dots\dots\dots..x_t$, form a reduced residue system modulo b (where $t = ø(b)$)then so do $ax_1, ax_2 \dots\dots.., ax_t$ in particular. The numbers $ax_1, ax_2, \dots\dots.., ax_t$ are congruent in some order to the numbers $x_1 x_2 \dots\dots, x_t$ we do not know exactly how these elements match up, but certainly if we multiply all the congruence together and sort things out, we get or

$$ax_1 ax_2 \dots ax_t \equiv ax_1 ax_2 \dots x_t\ (mod\ b),$$

$$a^{ø(b)}(ax_1 ax_2 \dots x_t) \equiv ax_1 ax_2 \dots x_t (mod\ b)$$

The product of the integers x_i is relatively prime to b and so the cancellation theorem yields.

Theorem: (3.22)

$$a^{ø(b)} \equiv 1\ (mod\ b)$$

If a and $b > 0$ are relatively prime integers, then:

$$a^{ø(b)} \equiv 1\ (mod\ b)$$

combining Euler's theorem with the last line if Theorem we get the following result .

Theorem (3.23):

If a and $b > 0$ are relatively prime integer and if k is the order of $a$modulo b, then $k|\emptyset(b)$.

Let us use Euler's theorem to find the last digit of 17^{102} what we are after is the least residue of $17^{102}\ (mod\ 10)$. Now$ø(10) = 4$, so by Euler's theorem:

$$17^{4} \equiv 1\ (mod\ 10)$$

Then

$$17^{102} = 17^{4.25+2} = (17^{4})^{25}17^{22} \equiv 1^{25}7^{2} = 49 \equiv 9(\ mod\ 10)$$

Thus the last digit 9.

Now suppose we want the last two digits of 17^{102} . Thus will be the least residue of $17^{102}(mod\ 100)$. Since $ø(100) = 40$, Euler's theorem tells us that:

$$17^{102} = 17^{40\cdot 2+22} = (17^{40})^{2}17^{22} \equiv 1^{40}7^{22} \equiv 17^{22}(\ mod\ 100)$$

Although we have reduced the exponent from 102 to 22 this still leaves us with a nasty computation. The integer 17^{22}has 28 digits and an ordinary calculator will give it in scientific notation, obscuring that last two digits. Ofcourse we could compute

$$17, 17^{2} = 189 \equiv 89, 17^{3}, = 17, 17 \cdot 17^{2} = 17 \cdot 89 = 1513 \equiv 13, \text{ect}$$

Reducing modulo 100 as we go until us it 17^{22}, but this would be tedious .In the next section,we will givean efficient method of doing such a calculation.

Fermat's theorem:

The case of Euler's theorem when the modulus is a prime p is attributed to Fermat. Actually Fermat merely told people he had proved the theorem bearing his name, Euler first publisheda proof. Since$\emptyset(p) = p - 1$ we have the following theorem.

Theorem (3.24): (Fermat theorem):

If p is prime and a is integer such that $p \nmid a$. Then:

$$a^{p-1} \equiv 1 \ (mod \ p)$$

of course, since p is prime $(a, p) = 1$ |is equivalent to $p \nmid a$ a slight variation allows this theorem to be stated with a simpler hypothesis.

Theorem (3.25): Fermat's theorem, second form) :

If p is prim, Then $a^p \equiv a \ (mod \ p)$ for all integers a

Proof:

If $p \nmid a$ then multiplying the congruence of the first form of the theorem by a gives the conclusion. But if p/a. Then both sides of the new congruence are congruent to 0modulo p.

Wilson's theorem:

The argument used to prove Euler's theorem above is too good to let alone recall that we derived the congruence

$$x_1 x_2 \dots \dots \dots \dots \dots . x_t \equiv a x_1 a x_2 \dots \dots \dots \dots \dots . a x_t \ (mod \ 6)$$

where $(a, b) = 1$, from the fact that if $x_1, x_2, \dots \dots \dots \dots ., x_t$ was a reduced residue system modulo b, then so was $ax_1, ax_2 \dots \dots \dots \dots ., ax_t$ matching up is the germ of this proof , i.e matching element x with congruent element ax, let us try to evaluate $(mod \ b)$ the product $x_1 x_2 \dots \dots \dots . x_t$ itself by a similar argument. By Theorem (3.6) we know that for each x in a reduced residue system $(mod \ b)$ there exists aunique element x' in the system such that

$$xx' \equiv 1 \ (mod \ b) .$$

our idea will be to pair up the elements x in this way each pair multiplying to $1 \ (mod \ b)$.

we seem to have proved that $x_1 x_2 \dots \dots \dots \dots . x_t \equiv 1 \ (mod \ b)$, but a little care is needed we must consider the possibility that x pairs with or self, that is , $xx \equiv 1(mod \ b)$. This is certainly the case if $x \ \equiv \pm 1 \ (mod \ b)$, and perhaps for other values of x for example $4 \cdot 4 \equiv 1\ (mod\ 15)$ If we assume the modulus is a prime p we simplify the situation, since if $x^2 \equiv 1\ (mod\ p)$.

Then $p/x^2 - 1 = (x-1)(x+1)$. Then Theorem (1.8) says that p divides one or the other of $x - 1$ and $x + 1$ and so $x \equiv \pm 1\ (mod\ p)$

A prime, modulus also has the advantage of every explicit reduced residue system, namely, $1,2, \dots \dots, p-1$. If $p = 11$, for example we can pair off everything except 1 and $10\ (\equiv -1)$. Indeed.

$$2 \cdot 6 \equiv 3 \cdot 4 \equiv 5 \cdot 9 \equiv 7 \cdot 8 \equiv 1\ (mod\ 11)\ .$$

Thus:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = \ 1(2 \cdot 6)\ (3 \cdot 4)(5 \cdot 90)(7 \cdot 8)10$$
$$\equiv -1\ (mod) 11).$$

The same argument works for any odd prime p, producing a theorem that bears John Wilson's name, even though there is evidence that Wilson (1741-1793) did more than guess it from numerical evidence . The first published proof was by langrage.

Theorem (3.26) (Wilson's theorem):

If p is prime. Then $(p-1)\ ! \ \equiv -1\ (mod\ p)$.

The statement (Wilson proof) of this theorem was first published by the English mathematician Edward warring in 1770 in his, meditations Algebraic, along with two other know as warning's problem, say that each positive integer is the sum of at most 4 squares, of almost 9 cubes, etc. That is, given appositive integer k is the sum of at most $g(k)$ the powers, A proof that $g(2) = 4$ appears in section (Lagrange first proved this) warnings problem as not settled in general until 1909, when the German mathematician David Hilbert proved it (Hilbert did not give a formula for $g(k)$, but merely showed it always existed) the other conjecture, due to Christian Gold Bach, says that each even integer greater than 2 can be written as the sum of two primes.

This still unproved Gold Bach conjecture is discussed in chapter 0.

Primality Testing:

The contra positive of Fermat's Theorem

By Fermat's theorem, if n is prime and n/a, then $a^{n-1} \equiv 1\ (mod\ n)$

Thus if $a^{n-1} \not\equiv 1\ (mod\ n), n$ cannot be prime. This idea has interesting consequences, pretend we do not know if 33 is prime or not, if it were prime,Then since 33 ∤ 2 we would have $2^{32} \equiv 1\ (mod\ 33)$. but in fact,

$$2^{32} = (2^5)^6 2^2 = 32^6 2^2 \equiv (-1)^6 2^2 = 4\ \ (mod\ 33).$$

Thus we have proved 33 in mot prime. Without exhibiting a factor between 1 and 33. This looks like a promising way to distinguish primes from composite and still satisfy the conclusion of Fermat's theorem. Since telling which even integer are prime is easy enough, let us look at odd values of n. we take $a = 2$ for simplicity, and compute the least residue r of $2^{n-1}(mod\ n)$.

n	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
r	1	1	1	4	1	1	4	1	1	4	1	16	13	1	1	4

From this limited evidence we might conjecture that the converse of Fermat's theorem is also true, at least for $a = 2$, that is , that if $2^{n-1} \equiv 1\ (mod\ n)$, then n is prime. Even if this is correct, however, it would be of limited use in determining the primality ofa large value of n without a more efficient way to compute 2^{n-1} . The computation of $2^{32}\ (mod\ 33)$ above was facilitated by noticing that 33 was exactly 1 more then 32, a power of 2 this trick will not work in general.

Our point of view is that n is so large that we do not know if it is prime or not, thus we cannot use Euler's the prime to simplify the calculation of 2^{n-1}since computing $ø(n)$ in any efficient way requires knowing the factorization of n into primes, and that is precisely what we do not know! .

We can always go back to deciding if the odd integer n is prime by checking it for divisibility by odd integers $\leq \sqrt{n},$ (Although we really only need to check possible prime divisors, determining whether a large possible divisor is prime needs fewer steps. Hen this to be worth considering. computing$2^{n-1}\ (mod\ m)$ by starting with 2 and multiplying $n - 2$ times by 2 , reducing modulo n as we go, takes $n-2$ multiplications and the same, number of divisions, and so is not acceptable.

Fortunately there is much more efficient way of computing powers modulo n suppose we wish to compute $a^d(mod\ n)$. As an example, we will compute the least residue of $848^{187}(mod\ 1189)$,

So that $a = 848, d = 187,$ and $n = 1189$. Thus seems to be a formidable task, but we will show how to do it using only aliened calculator we start by concerting the exponent d to its base 2, or binary representation. An easy way to do this is to successively divide d by 2, keeping track of the remainders (all of which are 0, or1) for $d = 187$ we have.

$$187 \equiv 93 \cdot 2 + 1$$
$$93 \equiv 46 \cdot 2 + 1$$
$$46 \equiv 23 \cdot 2 + 0$$
$$23 \equiv 11 \cdot 2 + 1$$
$$11 \equiv 5 \cdot 2 + 1$$
$$2 \equiv 1 \cdot 2 + 0$$
$$1 \equiv 0 \cdot 2 + 1$$

Then the remainders, listed in reverse order, give the binary representation of d. In our example:

$$d = 187 = 10\ 11\ 10\ 11_2$$
$$= 1 \cdot 2^7 + 0 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^2 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1$$
$$= 128 + 32 + 16 + 8 + 2 + 1$$

Now in order to compute a to the power $(mod\ n)$ we use the calculator to successively square and reduce n as follows. (*A*method for finding leasr residues with a hand calculator is given at the end).

k	$a^k\ (mod\ n)$
1	848
2	$848^2 \equiv 719,104 \equiv 948\ (mod\ 1189)$
43	$948^2 \equiv 898,704 \equiv 1009\ (mod\ 1189)$
8	$1009^2 \equiv 1,018,081 \equiv 297\ (mod\ 1189)$
16	$297^2 \equiv 88,209 \equiv 223\ (mod\ 1189)$
32	$223^2 \equiv 49,729 \equiv 980\ (\ mod\ 1189)$
64	$980^2 \equiv 960,400 \equiv 877\ (\ mod\ 1189)$
128	$877^2 \equiv 769,129 \equiv 1035\ (mod\ 1189)$

Then we have:

$$848^{187} = 848^{128+32+16+8+2+1}$$

$$= 848^{128}848^{32}848^{16}848^{8}848^{2}848^{1}$$

$$= 1035 \cdot 980 \ \cdot 223 \ \cdot 297 \ \cdot 948 \ \cdot 848 \ \ (mod\ 1189)$$

By multiplying out the last expression factor by factor, reducing modulo 1189 as we find

$$848^{187} = \ 190\ (mod\ 1189)$$

Example (3.27):

Compute the least residue of 2^{240} $(mod\ 341)$ using this method the reader should check the details of the example with a calculator or computer. We find

$$340 \ = \ 101010100_2$$

$$= \ 256 \ + \ 64 \ + \ 16 \ + \ 4\,.$$

Now

$$2^1 \equiv 2, 2^4 \equiv 16,$$

$$2^8 \equiv 256, 2^{16} \equiv 64, 2^{32} \equiv 4, 2^{64} \equiv 16, 2^{128} \equiv 256, and\ 2^{256} \equiv 64,$$

All modulo 341,.Thus:

$$2^{340} = 2^{256+64+156+4} = 2^{256}. 2^{64}. 2^{16}. 2^4 = \ 64.16.64.16 \ \equiv 1(mod\ 341)$$

The explain what we mean in saying the above modular exponentiation algorithm, is “efficient” we must take about computational complexity, a subject that has become important because of computers we would like estimate the number of steps a given algorithm

Takes. Actually what we will count will be the elementary aoperations of addition, subtraction multiplication, division and comparisons. Although the size of the numbers involved may affect how long such an operation takes an a computer, to keep things simple we will assume each such operation takes the same amount of time, say one. Billion of a second.

Of course, the number of elementary operations in an algorithm depends on the modular exponentiation algorithm. This size is measured by$d$, the exponent, we startby converting d to binary by divisions by 2 each division determines a binary digit suppose. There are k of these, namely $a_0, a_1, \dots \dots, a_{k-1}$ so that $d = a_{k-1}2^{k-1} + a_{k-2} + 2^{k-2} + \cdots + a_1 2 + a_0$ with $a_{k-1} = 1$. Note that $d \geq 2^{k-1}$. this part of the algorithmrequires k divisions. There are also K comparisons, Since after each divisionwe must check if the quotient is 0 to decide when to stop.

Now we compute $d^{2^1}, d^{2^2}, d^{2^3} \dots \dots \dots \dots, d^{2^{k-1}}$ $(mod\ n)$successively squaring and reducing modulo n (ire dividing by n and taking the remainder).

This accounts for $k - 1$ multiplications and $k - 1$ divisions.

Finally, we have at most k integers whose product we must compute$(mod\ n)$ need are at mist $k - 1$ more multiplications and $k - 1$ divisions. Our analysis has accounted for $2k + 2(k - 1) + 2(k - 1) = 6k\ - 4$ elementary operations. We had $2^{k-1} \leq\ d$, so$k - 1 = log_2 2^{k-1} \leq log_2 d$, which implies

$$6k - 4\ \leq\ 2 + 6\ log_2 d.$$

Theorem (3.28):

Let $a\ , b > 0$ and $n > 0$be integers . Then the least residue of a^d modulo n can be computed with no more than $2 +\ 6\ log_2 d$ elementary operations.

In the next section, we will consider computing a^d $(mod\ n)$ with $d \approx 10^{300}$ this could be done with no more than$2 +\ 6\ log_2 10^{300}\ \ = \ 2 + 6 \cdot 300 log_2\ 10 \approx$ 598 1 elementary operations (note that) $log_2 10 = 1/log_{10} 2 \approx 3 \cdot 322)$ compare this with computing $a^2, a^2, \dots \dots \dots .., a^d,$ reducing modulo n after each n after each multiplication .. There would about 2.10^{300} elementary operation, and the sun soul dot before ac computer doing one billion per second finish.

Interest in how many steps algorithm takes predates computers the following term was proved in 1844 by Gabriel lame'.

Lame's theorem:

If the Education algorithm us applied to two positive integers of then the number of divisions will not exceed 5 times the number of decimal digits of the smaller.

Proof:

Assume $0 < a < b$ and let the Euclidean algorithm m be applied as

$$b = aq_1 + r_1, \qquad 0 < r_1 < a$$

$$a = r_1 q_2 + r_2, \qquad 0 < r_1 < r_1$$

$$r_1 = r_2 q_3 + r_3, \qquad 0 < r_3 < r_2$$

$$r_{n-2} = r_{n-1} q_n + r_{n,}, \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1},$$

Not that$q_i \geq 1$ for $1 \leq i \leq n$, while $q_{n+1} \geq 2$, since q_{i+1} implies that $r_{n-1=} r_n$this proof will use the Fibonacci numbers$f_1 = 1, f_2 = 1, f_3 = 2,$ sincer_n is the last nonzero remainder,

$r_n \geq 1 = f_2$Because$q_{n+1} \geq 2$ we have $r_{n-1} \geq 2. r_n \geq 2 = f_3$

Likewise, using the Education algorithm equations and $q_i \geq 1$ we have

$$r_n - 2 \geq r_{n-1} + r_n \geq f_3 + f_2 = f_4,$$

$$r_n - 3 \geq r_{n-2} + r_{n-1} \geq f_4 + f_3 = f_5,$$

And in general $r_n - t \geq f_{t+2}$ taking t to be $n-2$ gives $n-2$ and $n-1$ gives $r_2 \geq f_n$ and $r_1 \geq f_{n+1}$

$$r_2 \geq f_n \text{and} r_1 \geq f_{n+1}$$

Thus

$$a \geq r_1 + r_2 \geq f_{n+1} + f_n = f_{n+2}$$

from this and Theorem (1.4) we have$a > A^n,$ where $A = (\sqrt{5} + 1)/2$

Note that $log\, A > {}^1\!/_5$. Supposea has k decimal digits, so that $< 10^k$.

Then

$$k = log_{10} 10^k > log_{10} a > log_{10} A^n = n log_{10} A > {}^n\!/_5$$

Thus $n < 5k$ since n and $5k$ are integers $n + 1 \leq 5k$. This concludes the proof, since $n + 1$ is the number of divisions in the Euclidean algorithm.

Now we return to the question of whether

$$2^{n-1} \equiv 1 \ (mod\, n\,)$$

Is not only a necessary condition for n to be prime, by Fermat's theorem, but s also sufficient? The ancient Chinese believed. This to be true.

The question has already been answer- did you catch it? In an example earlier in this section illustrating the modular exponentiation algorithm, we compute

$$2^{340} \equiv 1\ (mod\ 341).$$

This has the form of (3.5) with $n\ =\ 341$. But is not prime: $341\ = 11 \cdot 31$. Thus the dorm of (3.5) can be used to identify compose numbers but not primes. None the less, numbers like 341 are rare.

Definition (3.29): (pseudo prime, pseudo prime to base a)

We call ana pseudo prime if $2^{n-1} \equiv 1$ (mod n) is composite more generally, a composite numbers n such that $2^{n-1} \equiv 1$ (mod n) is called a pseudo prime to base a.

The a smallest pseudo prime is 341, and was not discovered until 1819 so the Chinese could pseudo prime for their assumption. Of course, bases other than 2 may also be used to identify composite to numbers for example,

$3^{340} \equiv 65\ (mod\ 341)$provinga factors less proof that 341 is not prime. Although there are infinitely many pseudo primers to base 2 (see the problems at the end of this section). They are much rarer than primes. Thus if a randomly chosen integer n satisfies (3.5), it is probably prime. Even rarer are pseudo primes to multiple bases. For example, there are only 1770 integersbelow $25 \cdot 10^9$ that are simultaneously pseudo primes to the bases $2.3{,}5$ and 7 . Thus the primelityof numbers less than $25 \cdot 10^9$could be determined by testing Fermat's congruence with these four bases, then comparing any number passing all four tests with a list of the 1770 exceptions. We might hope that for any composite number n, there is some base a for which Fermat's theorem could be used to show that n is composite we hope in vain: There are composite integers, called Carmichael numbers, which are pseudo primes to every base.

That is ,n is composite, but $561 = 3 \cdot 11 \cdot\ 17$ .It was only proved in 1994,by Al ford, Granville,andpomerance, that there are infinity many Carmichael numbers. Their proof was based on a suggestion of PaulErdős.

By using Fermat's theorem with multiple bases to weed out most composite numbers, and then more sophisticated tests, the primality of numbers of up to 150 digits can be determined in a few seconds with a computer. For integers of a special fro, such as mergenceandFermat numbers, even better methods are available, enabling the primedity of for larger numbers to determine. The lucas. Lember that, which has been used to identify many mersenne primes, is century, spanning theorem, since the 1878 lest of the Frenchman Eduard lucas was simplified by the American $s_1, s_2, \dots.$ by$s_1 = 4$ and $s_n = s_{n-1}^2 - 2$ for n> 1 , for example, $s_2 = 4^2 = 4^2 - 2 = 14$ and $s_3 = 14^2 - 2 = 194$. The test says that if p is an odd prime, Then $m_p = 2^p - 1$ is prime if and only if $s_{p-1} \equiv 0(mod\ m_p)$ as and example take $p = 7$, so $m_p = 2^2 - 1 = 127$ then

$$s_1 = 4, s_2 = 1, s_3 = 194 \equiv 67, s_4 \equiv 67^2 - 24487 \equiv 42$$

$$s_5 \equiv 42_2 - 2 - 1762 \equiv 111, \text{and} s_6 \equiv 111^2 - 2 = 12319 \equiv 0,$$

with all congruence modulo127. This proves that 1227 is prime.

An analogous test for Fermat numbers is the following.

Theorem (3.30): (pepims test):

If $n\ > 0$. The Fermat number $fn = 2^{\mathrm{a}^{\mathrm{n}}} + 1$ is prime if and only is

$$3^{(f_n - 1)/2}\ \equiv -1\ (mod\ f_n)$$

Proof:

We will only prave the "if" part here but a proof of the "only" part is in the problem for section asum. Then if p is any prime dividing fn we have $3^{(f_n - 1)/2} \equiv 1\ (mod\ p)$ by part (6) of theorem $(o\ p \neq 3)$, and squaring gives

$$3^{(f_n - 1)} \equiv (mod\ p).$$

Let k be the order of 3 modulo pTheorem (3.24) says that k divided$f_{n-1} = 2^{2^n}$. Thus $k = 2^t$ for some integer t$\leq 2^n$, suppose $t\ < 2^n$.

Then we can raise both sides of the congruence $3^k \equiv 1$ (mod p) to the power

$2^{2^{n-t-1}} \geq 1$ to get

$$1 \equiv (3^k)^{2^{2^n-t-1}} = 3^{2^{t(2^{2^n-t-1})}} = 3^{2^{2^n-1}} = 3^{\frac{2^{2^n}}{2}} = 3^{\frac{F_n-1}{2}} \equiv -1\ (mod\ p)$$

But this means $p = 2$, which is impossible. We must have $t = 2^n$and $k = 2^{2n} = fn - 1$. Now by Fermat's theorem $k \leq p - 1$, Thus $p \ \geq \ k + 1 \ = \ F_n$. Since p is a divisor of F_n, we must have $p = F_n$. Thus F_n is prime.

Example (3.31):

Usepepsin's test to show that $f_3 = 257$ is prime by the part of pepin's test provedabove; it suffices to show that

$$3^{(257-1)/2} = 3^{123} \equiv -1(mod\ 257).$$

But

$$3^2 \equiv \ 9, 3^4 \equiv \ 81, 3^8 \equiv 81^2 \equiv 136,$$

$$3^{16} \equiv \ 136^2 \equiv 249, 3^{32} \equiv 249^2 \equiv 64, 3^{64} \equiv 642, and 3^{128} \equiv 241^2 \equiv 256 \equiv -1$$

with all congruence's modulo 257. As we have seen, Format's theorem may tell us that a number is composite without providing a factor. In fact, factory appears to be much harder. (In terms of computation time. Then determining primality. Althoughmethods have been developed that are concededly better than trying all divisors up to the square root of the number to be factored. They are not powerful enough to factor, say, am arbitrary 300-digit number in any reasonable amount of time In 1994 a group at bellicose in Red bank. Now heresy, announced the factorization of a 129- digit number into two huge primes. The fact which took 8 amounts and was aided by the computes of 600 interest volunteers may have been the largest computation everat the time factoring the number had been set as a seemingly impossible task in a 1977 scientific American Column by math Gardner.

Public-key Cryptography:

The Idea of a key:

Cryptography is a method of sending a message in a farm that only its intended recipient can understand. Although this calls to mind spies, diplomats, and the military, cryptography has wider application. In an age even more and more information is transmitted over telephone lines or by radio (and so is subject to interceptionkeeping one's message (and credit card number) secret is an increasing problem for everybody.

Like everything else, cryptography has its own special language the original message is called the plaintext, and the (supposedly) unreadable version of it is called the cipher atext. The processes of going from plaintext to cipher text and back are called enciphering, respectively. Often enciphering methods involve a key that is known to the sender and intended receiver of the message but no one else. The idea is that someone who does not know the. The key will not be able to decipher the message even if he or she knows the general method of decipherment. We will illustrate the idea of a key with as substitution cipher, one of the oldest and simplest methods substitution amounts to merely replacing each letter of that alphabet with another letter. Although any messages if a few sentences or more enciphered by substitution may be easily figured out (in fact, such problems appear in newspapers and puzzle magazine), our aim with the example is simply to show the concepts involved. We will use as our key the words "number theory". first, we cross out any repeated letters leaving.

Now we write these letters nude' .The alphabet followed by the unused letters of the alphabet, in order.

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher text : N U M B E R T H B Y A C D F G I J K L P Q S V W X Z

To encipher we merely re [lace each letter of our message with the corresponding cipher text letter. Suppose or message is send money. We would replace. The S by L, since l is below S in our table, etc, we get.

Plaintext: SEBD MONEY.

Cipher text$L$: LEFB DGFEX

Of course to decipher LEFB DEGFEX the intend receiver of the message would use the key to make his own table like the one above , He would then use it in reverse, changing L to S, E to E,E to N , etc. to receive the original message.

CHAPTER FOUR
CONGRUENCIES WITH PRIME MODULE AND QUADRATIC RESIDUES

Just as an algebra goes from the study of linear equations to these involving higher of the unknown so also we proceed from the study of linear congruencies to the se of higher degree. Complications arise however. As we will see.

Polynomial congruencies:

We will consider polynomial congruencies in a single unknown. For

Example (4.1):

$$5x^4 + 17x^3 - 3x \pm 2 = 2x^3 - 7(mod 18)$$

In the from

$$F(x) \equiv 0(mod\ m).$$

Where $F(x)$ is a polynomial in x with integer coefficients?

Ourexample could be put in this byshifting everything to the left of the congruencies sign, so that

$F(x) = 5x^4 + 15x^3 - 3x + 9$ byTheorem if. $a \equiv \grave{a}(mod\, m)$, then $ax^k \equiv a\, x^k\ (mod\, m)$ for all integer Thus coefficient of $F(x)$ may be replaced by congruent coefficients without changing the set of solutions for example,

$$5\, x^4 + 15x^3 - 3x + 9 \equiv 0(\text{mod } 9)$$

is equivalent to

$$5\, x^4 + 6x^3 - 3x \equiv 0(\text{mod } 9)$$

Any term of $f(x)$ having coefficient divisible by the modulus many barhopped completely, since it is congruent to o no matter what x is. These considerations motivate the following.

Definition (4.2):

Degree of congruence if $f(x)$ is polymemial in x with intrgrat confficents, then by degree of the congruence $f(x)$ is, polynomial in x with integrat coefficcents , then by degree of the congruence $f(x) \equiv o\ (mod\, m)$.

We mean exponent of the highest power of x in $f(x)$ whose coefficient is not divisible by m.

Example (4.3):

Let $f(x) \ = \ 6x^3 \ + x^2 \ + \ 8$ then the degree of x in $f(x) \equiv \ 0 \ (mod \ m)$.

if $m \ = 5$ but if $m \ = 3$ then the degree is only 2.

The values $x \ = \ 0, 1, 2, 3, 4$ as follows.

x	0	1	2	3	4
$f(x)$	8	15	60	179	408

This a complete solution is $x \ = \ 1$,2(actually it would to test the values $x = -2, -1 \ , 0 \ , 1 \ , 2$).

Another complete solution is $x \ = \ 42$,16 (since $42 \ \equiv \ 2$ and $16 \equiv I \ (\ mod \ 5)$.

Reducing a congruence to prime power modnli consider the congruence $f(x) \ =$

$$6x^3 \ + \ x^2 \ 8 \ \equiv \ 0 \ (\ mod \ 20).$$

Solving this by trial – and –error would finder evaluating $F_{(x)}20$ integer a tedious task there is Avery to refuse the work.

Recall that the come says that if $(b_1, b_2) \ = \ 1$, then $Z \equiv \acute{Z} \ (mod \ b_1 b_2)$ if end only

$$Z \equiv \ \acute{Z} \ (mod \ b_1) \text{ and } Z \equiv \acute{Z} \ (mod \ b_2).$$

Appling this theorem with $Z \ = \ f(x) \ , \acute{Z} = 0, \ b_1 \ = \ 5$ end $b_2 \ = \ 4$ we see that $f(x) \ \ \equiv 0(\ mod \ 20)$ is equivalent to

$$f(x) \ \ \equiv 0(mod \ 5) \text{ and } f(x) \ \ \equiv 0 \ (mod \ 4) \ .$$

We solved the congruence with modulo 5 the lest example, finding that $x \ = \ 1, 2$ was a complete solution. From tinetable solution for the modulus 4. Then x is a solution to the original congruence if end only if $x \equiv 1$ or $2 \ (mod \ 5)$ end $x \ \equiv \ o$ or $2 \ (mod \ 4)$. solving these simultaneous congruence in section.

Each fair of solutions module 4 and 5 generates unique solution modulo 20, so we get four (2 times 2) solutions in all.

The reader should review the Chinese remainder theorem and confirm that x satisfies if and only if $x \ \equiv \ 2, \ b$,12,or $1b \ (mod \ 20)$.

Thus this is a complete solution to the or inguinal congruence voice that in order to apply theorem and the Chinese remainder theorem the smaller module employed must be relatively prime. Thus factoring 20 into 4 times 5 worked, but 2 times 10 would not have, since 2 and 10 are not relatively prime.

This method may be used to simplify the solution of

$$f(x) \equiv 0\ (mod\ m)\,.$$

Whiner m can be factored into relative by prime smaller factors, that is, whenever more than one prime divides m. More than two factors may beused. For example, $f(x) \equiv 0\ (mod\ 360)$ may be replaced by $f(x) \equiv (mod\ 9)$ and $f(x) \equiv 0\ (mod\ 40)$.

But the left congruence is equivalent to $f(x) \equiv (\ mod\ 8)$ and smaller pieces the modulus can be broken into are the prime powers in it's factorization.

This method is summarized in the following theorem. The details of the proof (aversion of theorem U. s More than two modulo is needed for example: are left for the exercises.

Theorem (4.4):

Consider the congruence $f(x) \equiv (\ mod\ m)$.

Where F is o polynomial with integer coefficients and m is positive integer.

Let

$$m = p_1^{n_1} p_2^{n_2} \ldots . p_r^{n_r}$$

Where $p_1\ , p_2, \ldots \ldots \ldots , p_r$ are distinct prime. Suppose o complete solution to $F(x) \equiv O\ (mod\ p_i^{n_i})$.

Has be elements, $= 1\ , 2, \ldots \ldots\ r$. Then a complete solution to the original congruence has$k_1 k_2\ \ldots . . k_r$elements.

In fact, if for each$i = 1\ , 2 \ldots r, x_i$ is a solution to $F(x) = 0\ (mod\ p_i^{n_i})$

Then any x such that $x \equiv x_i\ (mod\ \ p_i^{n_i})\ ,\ i = 1\ ,\ 2\ , \ldots . , r$ satisfies the original congruence, and a complete solution to it may be constructed this way by allowing the x_i to run through complete solutions to the congruence with prime power module.

Example (4.4):

Solve

$$3x^2 - 20\,x + 25 \equiv 0\ (mod\,84).$$

The power facers of 84 are 4, 3 and 7.

By testing in complete residue systems we find that a complete solution to $3x^2 + 1 \equiv 0\,(mod\,4)$ is $x = 1\,,3$ a complete solution to $x + 1 \equiv 0\,(mod\,3\,)$ is $x = -1$; and a complete solution to $3x^2 + x + 4 \equiv 0\,(mod\,7)$ is $x = -3\,,-2$(note that the congruence have been is amplified by reducing coefficients, depending on the modulus.)

Now we use the Chinese remainder theorem to solve the simultaneous congruence

$$x \equiv 1 \text{ or } 3\ (mod\,4)$$

$$x \equiv -1 \quad (mod\,5)$$

$$x \equiv 3 \text{ or } -2\ (mod\,7)$$

Which involves solving

$$21\,x_1 \equiv 1\ (mod\ \ 4),$$

$$22x_2 \equiv 1\ (mod\ \ 3),$$

$$12\,x_3 \equiv 1\ (mod\ \ 7),$$

Solutions are $x_1 = 1,\ x_2 = 1$ and$x_3 = 3$. Them the simultaneous solution is

$$x = 21\,(1)\,(\,1 \text{ or } 3) + 22\,(1)(-1) + 12\,(3)\,(\,-3 \text{ or } -2)$$

$$= -115, -79, -37\,,73.$$

This is a complete solution to the original congruencies the lost complete solution is $x = 5, 11, 47\,,53$.

Example (4.5):

solve $x^2 + 1 \equiv o\ (mod\ 35)$.

By trial we find that of the two congruencies $x^2 + 1 \equiv o\ (mod\,5)$ and $x^2 + 1 \equiv O\ (mod\,7)$, $x = -2\,,2$is a complete solution to the first, but the second congruence has no solution 5 either.

This illustrates that in theorem some of the numbers ki may be zero.

Congruencies with modulus p^2:

The above method doesnot help with the congruence

$$2x^3 - 3\,x + 6\ \equiv 0\ (mod\ 25),$$

Since only one prime divides the modulus.

It is possible to avoid testing 25 values of x in it, however.

The method we will illustrate dependon the fact that part of theorem any solution to also satisfies 2 $x^3 - 3x +\ 6\ \equiv\ o\ (mod\ 5)$.

By testing$x\ =\ 2\ ,-1\ ,o\ ,1\ ,2$ we see it has acomplete solution$x\ =\ 1$.

Thus instead of trying all of $0\ ,1,\dots\ ,24$ we need only try values of

$x\ \equiv 1\ (mod\ 5),$ namely $x = 1, b,\quad 11,\quad 16,\quad$ and $21.$

Even these computations may be avoided. We want to testsolution of the form $x\ =\ 1\ +\ 5y$, where $y\ =\ 0\ ,1\ ,2\ ,3$ or 4 . subsuming this expression gives

$$2\ (\ 1 -\ 5y)^3 - 3\ (1\ +\ 5y) + 6 \equiv\ o\ (mod\ 25)$$

simplifying this algebraically and dropping those terms with coefficients divisible by 25 yields $15y\ +\ 5\ \equiv\ 0\ (mod\ 25)$.

By Theorem (1.19) (with $a =\ 5$ and $b\ =\ 25$) this is equivalent to

$$3y\ +\ 1 \equiv\ 0\ (mod\ 5).$$

Since we are interested in y ranging from 0 to 4 we want a complete solution one is easily seen to be $y\ =\ 3$.

We see that a complete solution to is $x =\ \ 1\ +\ 5\ (3)\ =\ 16.$

The method of this example works in general that is:given congruence

$$F(x)\ \equiv\ 0\ (mod\ p^2\ )$$

Where p is prime, we first solar $F(x)\ \ \equiv\ O\ (mod\ p)$ now it $\acute{x}$ is any solution to we look for solutions of the form $= \acute{x}\ \ + py$, where y is in some complete residue system medal $o\ p$.

Substituting this expression leads to linear congruence $ay\ +\ b\ \equiv 0\ (mod\ p)$ in y , to which a complete solution is desired.

The reason that turns out to be linear is that when $\acute{x}\ \ +\ p\ y$is raised to a power, most of the terms in evolving because they have a coefficient divisible by $p2$.

Onto that if has more than one solutions the succeeding process must be applied to cach of them.

This technique will be greaten baized and investigated in detail in this next section.

Congruencies with prime module:

Congruence the method power modal generating the method of the last section:

In the lost section, we saw how sowing any polynomial congruence can be rejoiced, with the help of the Chinese remainder theorem. To selling congruencies with would powers of frame, and at the end of the section method of solving congruence s with modulus p2 , was illustrated. We will generalize.

The later or the general plan, given congruence $F(x) \equiv O \ (mod\, p^{n})$,

Will be to find first a complete solution to

$F(n) \equiv O \ (mod\, p)$, then use this to solve

$$F\ (n) \equiv O\ (mod\, p^{2}),$$

And continue this way until we jars complete solution to the original congruence.

What we need is a method for going modulus p^{k} to modulus p^{k}+1 consider the congruencies

$$F(x) \equiv 0\ (mod\, p^{k})$$

And

$$F(x) \equiv 0\ (mod\, p^{k+1})$$

By the last part of theorem any solution is also a solution so $if\ \ x_k, \acute{x}_k, \acute{\acute{x}}_k$ … ..is complete solution of, then any solution of (4.9) will be congruent to one of these numbers $(mod\, p^{k})$.

Thus we can rest rick our attention to solution of the form

$$x_k + p^{k}y, \acute{x}_k + p^{k}y, \dots,$$

Where y is an integer.

Furthermore, we can assume that $y$is in some complete residue system $(mod\, p)$, since if $y \equiv \acute{y}\ (mod\, p)$, then it can be checked that $x_k + p^{k}y \equiv x_k + p^{k}\acute{y}\ (mod\, p^{k+1})$, and also these numbers could not both appear in complete solution to let us consider a particular solution x_k of and see what solutions of the form $x_k + P^k y$ of it might generate.

We wish to find out which y satisfy

$$F(x_k + P^k y) \equiv 0(mod\, P^{k+1})$$

let us assume$F\ (x) = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_0$.

Them atypical term on the left side of will be $aj\ (x^k + p^k y)^j$.

If this is multiplied out, an unpleasant expression of $j + 1$ terms will result, but fortunately it turns out that all but the first two will be divisible by p^{k+1}, and so may be dropped from the congruence.

Since the complexities of the expression involved may obscure what is going on, let us simplify the mutation.We claim that

$$(u + mv)^j = u^j - ju^{j-1}mv + (\text{a multiple of} m^2).$$

Forany integers u, m and v any positives integer j .

Although the binomial theorem could be invoked to prove this all that is really needed is to notice that the expression on the left is $u(mv)$ multiplied by itself j times , that is

$$(u + mv)(\ u + mv) \ldots\ (u + mv)$$

$$j \text{ factors}$$

In particular, if we take $u = x_k, m\ = p^k$, and $= \ y$, we see that

$$aj\ (x_k +\ p^k y)^j = a_j(x\,{}^j_k\ + jx\,{}^{j-1}_k\ \ p\,{}^k_y\ +\ a\text{multiple of } (p^{2k}).$$

Since it is easy to see that $2k\ \geq\ k + 1$ for k any positive integer, this means that in the congruence the term. in question may be replaced by

$$a_j x_k^j + a_j j x_k^{j-1} p^k y$$

By collecting the terms involving y we see that (4.10) my be written in the from $F(x_k) + F'(x_k)p^k y \equiv 0(mod\, p^{k+1})$ where $F'(x)$ is the polynomial

$$a_r r x^{r-1} +\ a_{r-1}\,(r-1)x^{r-2} + \cdots . + a_1.$$

Calculus students should recognize that this is just the derivative of $F(x)$. No calculus is really needed here, however, since it is enough to define $F'(x)$ in a formal way for any polynomial $f(x)$.

Definition (4.5):

derivative of a polynomial given a polynomial $F(x) = a_r x^r + \cdots + a_0$, we define it is (formal) derivative to be the polynomial

$$F'(x) = a_r\, r x^{r-1} + a_{r-1}(r-1)x^{r-2} + \cdots + a_1.$$

For example The derivative of

$$3x^5 - 4x^3 + 2x^2 + 9x + 14 \quad \text{is } 15x^4 - 12x^2 + 4x + 9.$$

Linear congruence for y:

We saw above that if $x_k$is a solution to, then $x_k + p^k y$ is solution to exact when

$$F(x_k) + F'(x_k)p^k y \equiv O(mod\, p^{k+1})$$

this congruence is equivalent to

$$\frac{F(x_k)}{pk} + F'(x_k)y \equiv O\ (mod\, p)\ or\ F'(x_k)\, y \equiv \frac{-F(x_k)}{pk}\ \ (mod\, p)$$

(Note That the tram on the right is an integer by the assumption that x_k satisfies. Thus finding 4 involves only solvingalinear congruence with modulus p. 13 e for summarizing this method in a theorem we illustrate it.

Example (4.6):

Solve $x^2 + x + 3 \equiv O\ (mod\ 27)$.

We testing by solving the congruence $x^2 + x + 3 \equiv O\ (mod\ 3\ )$.

By testing values of x in complete solutions $x_1 = -1,0$.

Solution to the congruence with modulus a will be of the form $x_1 + 3\,y$, where y satisfies

$$F'(x_1) \equiv \frac{-F(x_1)}{3}(mod\ 3).$$

Note that $F'(x) = 2x + 1$. For $x_1 = -1$, This congruence is

$$(-1)y \equiv \frac{-3}{3}\ (mod\ 3)$$

This has the complete solution $y = 1$, given $x_2 = -1 + 3(1) = 2$.

If we take $x_1 \ = \ 0$, then congruence is

$(1)y \ = \frac{-3}{3} \ (mod\ 3)$ which the complete solution

$$y \ = \ -1, \qquad x_2 \ = \ 0 + 3\,(-1) \ = \ -3$$

Now we look for solutions to the original congruence with modulus 21 of the from $x_3 = \ x_2 + \ 9\,y$.

Here y must satisfy $F'\ (x_2) \ \equiv \ \frac{-F(X2)}{9} \ (mod\ 3)$.

For x_2 2, This congruencies is.

$5\,y \equiv \ \frac{-9}{9} \ (mod\ 3)$, which has the complete solution $y = \ 1$,and so

$$x_3 \equiv 2 + 9(1) = \ 11.$$

Using $x_2 \ = \ 3$ gives the congruence $-5y \ \equiv \ \frac{-9}{9}(mod\ 3)$ which has the complete solution $y \ = \ -1$.

Thus here $x_3 \ = -3 \ + 9\,(-1) \ = -12$. Acomplete solution to the original congruence is $x \ = \ 11, -12$.

The least complete solution is$x \ = \ 11, 15$.

Theorem (4.7):

suppose $x_k\,, x_k'\,, x_k''\,, \ldots,$ is acomplete solution to the congruence $f(x) \ \equiv \ o\ (\ mod\ p^k)$. Where$F\infty$an integral polynomial and P is is a prime. Then all solution to $f(x) \ \equiv \ O(mod\ P^{k+1})$ in some complete resident system modulo P^{k+1} congruence to $x^k(mod\ P^k)$ are given by $x^{k+1} = x_k + P^k y$, where y runs through any complete solution to

$$F'(x_k)\,y \ \equiv \ \frac{F(x^k)}{p_k} \ (mod\ P).$$

Applying this also to $x_k'\,, x_k''$ ... in turn yields acomplete solution to

$$F(x) \ \equiv \ O\ (mod\ P^{k+1}).$$

Notice that according to Theorem The congruence $ax \equiv \ c\ (mod\ b)$ has a solution exist, then a complete solution has (a, b) elements.

In the case of the congruence defining y, we have the modulus b is p, and so (a, b) equals 1 for p.

Thus each solution $x_k$generates $0,1,$ or p solutions x_{k+1} at the next level.

Example (4.8):

solve

$$x^3 + x^2 + 23 \ \equiv \ O \ (mod \ 125).$$

We start with the congruence $F(x) \equiv 0(mod \ 5)$, where

$$F(x) = x^3 + x^2 + 23.$$

The following table shows that a complete solution $x_1 = 1 \, , 2.$

x_1	-2	-1	0	1	2
$F(x_1)$	19	23	23	25	35

Notice that $F'(x) = 3 \ x^2 + 2x$. We will find solution $x_2$to

$F(x) \equiv \ o(mod \ 25)$ of the form x_1 + 5y, where y satisfies

$$F'(x_1) \ \equiv \ \frac{-F(x_1)}{5} \ \ (mod \ 5).$$

For $x_1 \ = 1$, this congruence is $5y \ \equiv \ \frac{-25}{5}$ and a complete solution is

$$y \ = \ -2 \, , -1 \, , 0, 1 \, , 2.$$

Thus

$$x_2 = \ 1 \ + \ 5y \ = \ -9 \, , -4 \, , 1, 6, 11.$$

For $x_1 = \ 2$, the congruence for by becomes $16 \ y \equiv \ \frac{-35}{5} \ (mod \ 5)$, and a complete solution is $y \ = -2$ yielding $x_2 = 2 + 5y = -8.$

It is useful to make a table of fiend F1 for the values of x_2

x_2	-9	-4	1	6	11	-8
$F(x_2)$	-625	-25	25	275	1475	-425
$F^1(x_2)$	$\equiv \ 5$	$\equiv \ 5$	$\equiv \ 5$	$\equiv \ 5$	$\equiv \ 5$	$\equiv \ 16$

There the congruencies in lest line are modulo 5.

Notice in the congruence $F'(x_k) \, y \equiv \ \frac{-F(X_k)}{pk} (mod \, p)$ all that matters about $F'(x_k)$ is what it is modulo p.

Since all solutions x_k arising from a given solution x_1 need only be computed once for each of these. For example, all the solutions

$x_2 = -9\,,-4,1\,,6\,,11$ arising from $x_1 = 1$ will have

$$F'(x_2) \equiv 5\ (mod\ 5).$$

We must find new values of y satisfying $F'(x_2)\ y\ \equiv\ \frac{-F(X2)}{25}\ \ (mod\ 5).$

For

$X_2\ =\ -9\,,-4\,,1\,,b\,,11$, we get the congruencies

$$5y\ \equiv\ 25\,,\qquad 1,\qquad -1,-\,11,-5\ \ (mod\ 5).$$

Only the first of these is solvable, with the complete solution

$y =\ -2,-1\,,0,1,\ 2$, which yields

$$x_3\ \equiv\ -9\ +\ 25\,y = -59,-\,34,-9,16\,,41.$$

Taking $x_2 \equiv -8$ leads to the congruence $16\,y\ \equiv\ 17\ (mod\ 5)$ with the complete solution $y =\ 24$, which we gives $x_3 = -8 + 25y = 42$ solution to the original congruence is $X =\ -59\,,-34,-9,16,41,42$ the least complete solution is $x\ =\ \ I6,\ \ 41,\ \ 42,\ \ 66,\ \ 91,\ \ 116.$

Quadratic Residues Congruencies of Degree two:

In the previous two sections, we have seen how to reduce the solution of any polynomial congruence to that of congruence with prime module. For each congruency, however, our technique is to test the elements of a complete residue system.

Areas on cable way to start the analysis of such congruence would be to restrict their degree, since linear congruence were complete by covered in section we consider congruencies of degree two say

$$ax^2 + bx + c =\ o(\ mod\ p),$$

where p is prime.

The first thing that comes to wind on looking is the quadratic formula .This says that the solutions of the equation $ax^2 + bx +\ c =\ 0$ are given by

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

If we are interested only in real solution there will be 0,1 or 2 of them according as $b^2 - 4ac$ aces negative zero, or positive.

In the congruence we are looking for integral solution x.

Of can course, if $b^2 - 4ac$ is not a perfect square, than the radical will not be an integer (in May not even by real). Perhaps it would be sufficient for $b^2 - 4ac$ to be congruent to a square, say $y2$.modulo$p$. Then we might take $x = \frac{-b+y}{2a}$.

A problem still remains, name by, the division by $2ax \equiv b + y(mod\ p)$?

By Theorem this will exit whenever$(2a, P) = 1$ but we can assume that P does not divide a, since otherwise is not really a congruence of degree 2. Also if P divide2, then $P = 2$. We should be so lucky; solving congruencies with modulus 2 is a solution to the congruence. We might even dream that every solution to could be generated this way.

The strange thing is that is works! We have just seen an example of a type pervades mathematical creation yet almost never gets into print.

Although sometimes completely fruitless, less, such uncritical thinking often carries one dose enough to the truth Co direct the application of were rigorous arguments just as an illegal wiretap, while not admissible in court; way lead the police to construct a legitimate cues.

Theorem (4.9):

If , b and c are integers and p is an odd prime not dividing a, then the solutions of the congruence $ax^2 + bx + c \equiv o(modp)$ are given by the solutions $y^2 \equiv b^2 - 4ac$

A complete solution has 1 element if p proof.

To prove the first sentence we must show two things:

1. If $y^2 \equiv b^2 - 4ac$ and $2ax \equiv -b + y(mod\ P)$. then y is solution to the ordinal congruence.
2. Every solution to the original congruence is generating this way. As with the proof of the quadratic formula proving (1) more by involves substitution into the original congruence, and will be left for the exercises at the end of this section.

To prove (2) we also copy the corresponding part of the proof of the quadratic for mule, which involves completing the square.

Let us assume x satisfies the original congruence.

We multiply by u a to be sure that everything remains integral when we complete the square, getting $4a^2x^2 + 4acx + 4ac \equiv \ O \ (mod \ P)$, or

$$(2ax + b)^2 - \ b^2 + \ 4ac \ \ \equiv \ O \ (mod \ P),$$

If we how define y to be $2ax + \ b$ then we have from the last congruence that $y^2 \equiv \ b^2 - 4ac \ (mod \ P)$, and also that $2ax \equiv -b + y \ (mod \ P)$ from the definition of y.

Notice that by Theorem if y generated x and y' generated x' by this method, then $X \equiv x^1 \ (mod \ P)$ if end only if $y \equiv \ y^1 \ (mod \ P)$.

Thus to count the Clements in suffices to cant a complete solution to $y^2 \ \equiv y'^2 \ (mod \ p)$, subdivides $y^2 - y'^2 \ = \ (y - y') \ (y + y')$.

By Theorem this implies $y' \equiv y$ or $- \ y \ (mod \ p)$,

There are two solutions unless $y^2 \ \equiv b^2 - 4ac \ (modp)$,

which says p divides $2y$. since p is odd then , latter happens only when p divides y (and say), in which case there is only one solution.

But $y^2 \equiv \ b^2$– $4ac \ (mod \ P)$, which proves the last sentence of the theorem.

Example (4.10):

Solve $x^2 + 6x + 1 \ \equiv \ O \ (mod \ 31)$.

Here $a = 1, b = 6$, and $c = \ 1$. The obvious solutions to

$$y^2 \equiv b^2 - 4a \ c = 32 \ \equiv 1 \ (mod \ 31) \ are \ y \pm \ 1.$$

Then we must solve

$$2ax \equiv -b + y \text{ or } 2x \ \equiv -6 \pm 1 \equiv \ -5 \text{ or} - 7 \ (mod \ 31).$$

Solutions are is $x = 13,12$, and this is complete solution to the original congruence.

Clearly it is of integer to know for which numbers m the congruence $y^2 \equiv \ m \ (mod \ P)$ is solvable.

If P divides , as we have seen, $y = 0$ is a complete solution but if $P \nmid m$ hither a solution exists or not may not be obvious .

Definition (4.11):

Quadratic residue quadratic no residue let P be prime and suppose Pt a.

We call a quadratic residues moa duo P in case there exists an integer $y$such that $y^2 \equiv a(mod\, P)$. if no such y exists than we call quadratic non residues modulo P.

Example (4.12):

The integers 1 , 4 , and 12 are quadratic residues

$$(mod\ 13)\ (\text{not that } 5^2\ \equiv 12\ (mod\ 13)$$

while 2 is a quadratic nonresident (mod 5) since $y^2 \equiv 2\ (mod\ 5)$ has no solution.

Since if $a \equiv a'(mod\ P)$, then the congruencies $y^2 \equiv\ a\ (modp)$, and $y^2 \equiv a_1(mod\ p)$ are equivalent The quadratic residues make whole congruence classes. The argument at the end of the proof of the previous harem shows that if P is an old prime, if a, and if $y2\ \equiv\ a\ (mod\ P)$ is solvable, then there are exactly two elements in a complete solution, the other being congruence to $-y$. Thus if we complete

$$1^2, 2^2\ , 2^3, \dots . (p-1)^2$$

we hit each, congruence class $(mod\ P)$ containing quadratic residues exactly twice, first with some k, $1 \le k\ \le \frac{(P-1)}{2}$, and the second time with $p-k$, since $(p-k)^2 \equiv k^2(mod\ p)$. Thus we have the following theorem, which at least cuts down by half the task of looking for solutions to $y^2 \equiv a\ (mod\ p)$.

Theorem (4.13):

Let P be any odd prime. Then any reduced residue system modulo P contains $(p-1)/2$quadratic residues and $(p-1)/2$ quadratic no residues modulo p. One set of $(P-1)/2$ incongruence quadratic residues is $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$.

Example (4.14):

We compute the least residues $(mod\ 11)$ of k^2 , $k = 1,2,\ldots\ldots,10$, in the following table.

k	1	2	3	4	5	6	7	8	9	10
k^2	1	4	9	5	3	3	5	9	4	1

Note the each quadratic residue appears one between $k = 1$ and $5 = (11 - 1)/2$.

Example (4.15):

Solve $2x^2 + 3x + 5 \equiv o\ (mod\ 23)$.

Here b^2 - $4ac = 9 - 4(2)(5) = -31 \equiv 15\ (mod\ 23)$.

We complete the least residues $(mod\ 23)$ of the squares of the squares of the into or s from q to $(23 - 1)/2 = 11$ to get the following table. .

k	1	2	3	4	5	6	7	8	9	10	11
k^2	1	4	9	16	2	13	3	18	17	8	6

Letting k run from 12 to 22 would produce the same squares in reverse order. (Tryit!) Thus 15 is a quadratic nonresident $(mod\ 23)$ and the original congruence has no solution.

The reader may want to review the proof of Wilson's theorem, in which it is shown that $(p - 1)! \equiv -1\ (mod\ P)$by matching each of the integers k from $1, 2 \ldots\ldots, p - 1$ with integer $k'$from thus list such that

$$k^k \equiv 1\ (mod\ p).$$

We vary this proof as following. Suppose P is an old prime not dividing a, and match each k between 1 and $p - 1$ with a k^1 in that set such that

$$kk' \equiv 1(mod\ p).$$

Exactly one such k exists by Theorem. There is a problem with the count if we could have $k = k'$ which says $k^2 \equiv a\ (mod\ p)$.

This problemcannot arise if a is a quadratic nonresident $(mod\ p)$ so let us assume that such is the case for the time being.

Then we have $a^{(p-1)/2} \equiv 1 \cdot 2 \ldots (p-1) \equiv -1 \ (mod\, p),$, where of course , theorem.

We see that if a is a quadratic no residue $(mod\, p)$ we table a more direct approach. Let $y^2 \equiv \ a\ (mod\, p)$. Since $p \nmid \ a,$ also $p \nmid \ y$. Then $a^{(p-1)/2} \ \equiv \ y^{p-1} \ \equiv \ 1\ (mod\, p)$ by format's theorem.

Theorem (4.16) :

(Euler's criterion). Let P be an prime not dividing the integer a, Then a is a quadratic residue or quadratic no residue modulo p according as $a^{(p-1)/2} \equiv 1 \text{ or } -1\ (mod\, P)$ in light of the modular exponentiation of section , this theorem gives an efficient method of telling whether a given integer is a quadratic residue or no residue modulo p, although it dose not give an actual that $y^2 \equiv a\ (mod\, p)$ in the case of a quadratic residue the case $a \ = \ -1$ is especially pleasant, since powers of -1 are easily computed.

Corollary (4.17):

The number -1 is a quadratic residueor quadratic no residue modulo the odd prime p according as p is congruent to 1 or 3 modulo 4.

Proof of course, any odd prime p must be congruent to 1 or 3 modulo 4. And it is easy to check that then $(p-1)\ /2$ is even or odd irrespectively.

Definition (4.18):

Legendre symbol suppose pies an odd prime not dividing the integer a. We define the symbol $(a|p)$ to be $1or\ -1$ according as a is a quadratic residue or b quadratic no residue modulo. This is called the Legendre symbol, after the Frenchmathematician AdrianMarieLegendre (1752 - 1833).

Example (4.19):

Fromprevious examples, we see that $(1/13) = (4/13) = (12/13) = 1$, while $\left(\frac{2}{5}\right) = (15/23) = \ -1.$

Theorem (4.20):-

The Integra $\ a\ $ or $\ b.$

1) $\left(\frac{a^2}{p}\right) = 1$,

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

3) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(mod\ \ p)$.

4) If $a \equiv b\ (mod\ P)$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

5) $\left(\frac{-1}{p}\right) = 1$ or -1 according as $p \equiv 1$ or $3\ (mod\ 4)$

Proof:

Parts (1) and (4) follow airside. Part (3) is Euler's criterion, and part (5) is its corollary.

Finally, part (2) follows from pert (3) since

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right)(mod\ \ p)$$

Quadratic Reciprocity identifying Quadratic residues:

The problem of telling whether an integer a is a quadratic residue modulo P or not occupied some of the greatest number theorists of the eighteenth century, including Euler, leg range, Legendre and gauss who made the greatest contribution to the subject.

To save words we will establish the following contention convention in this section, p will represent an odd prime not dividing the positive integer$a$. All congruence will be modulo p unless some other modulus is specified.

Note that we can assume$a$ to be positive without loss of generality, since by part (2) of $(-a/\ p) = (-1/p)\ (a/p)$ and $(-1/p)$ can be evaluated by part (3) of the some theorem. About all w have to go on is Euler's criterion. Which says $\left(\frac{a}{p}\right) \equiv\ a^{(p-1)/2}$and it would be nice to have some independent way to evaluable the expression on the right . In the proof. Of Euler's theorem (her precession , showing that $a^{(p-1)} \equiv 1$ Recall the proof. As x runs through reduced residue system modulo p so does $a\ x$, so

$a^{(p-1)}\ \prod x = \prod(ax) = \prod x$, where the products run over

$$x = 1, 2, \ldots, p - 1$$

Dividing through by $\prod x$ yields formable theorem.

In order to valuate $a^{(p-1)/2}$wo need to employ product with $(p-1)/2$pastors, say over $x = 1, 2, \ldots, (p-1)/2$. Let us define the integers from 1 to p-1 then look like $1, 2, \ldots, \frac{p-1}{2} = h, , h+1 = \frac{p-1}{2}, \ldots, p - 1$.

A proof$4ke$ that for format's theorem would here us the product $a^h \prod x = \prod(ax)$, where x runs from1 To h in the products.

The problem with this product is that for x between 1 and h, ax need not be congruent to some number in the same range certainly in congruent to one of the number $-h, -(h-1), \ldots., -1, o, 1, 2, \ldots, h$ since these $2h + 1 = p$ integers comprise a complete residue system $(mod\ p)$. In fact, we would leave out O as a possibility, since by $(x)r$ assumptions $p \nmid ax$.

Let us define $x^*$to be that unique number between $-h$ and h such that $ax = x^*$ where x runs from 1 to h. Taking $p = 7$ and $a = 5$, for example, we compute the following table. Note that $h = (7-1)/2 = 3$.

x	1	2	3
ax	5	10	15
x^*	-2	3	1

Here is another example, with $p = 13$ (so $h - 6$) and $a - 2$.

x	1	2	3	4	5	6
ax	2	4	6	8	10	12
x^*	2	4	6	-5	-3	-1

Notice that the values of x^* repeat those of x, except for some minus signs. This turns out always to be the ease, which is the basis of the following theorem.

Theorem (4.21): Gauss's lemmas:

Let P be an old prime not dividing the integer a.

For $x = 1, 2, \ldots, h = (p-1)/2$ letx^*be that integer congruent to $ax\ (mod\ p)$ such that $-h \leq x^* \leq h$.

Suppose exactly n values of $x^*$are negative.

Then $(a\backslash b) = (-1)^n$.

Proof:

first we show that the a absolute values of the number x^*comprise the set $\{\, 1, 2, \dots, h\}$, Since these absolute velour all fall into this set, and show they are distinct, that is , if $x \neq y$, then $|x^*| \neq |y^*|$. Suppose $|x^*| = |y^*|$, with x and y by the cancellation theorem.

Otherwise $x^* = -y^*$, which means $ax = -ay$.

Thus $p|\ a\ (x + y)$. This is impossible because$x$ and y are between 1 and 4, so $2 \leq x + y \leq 2h = p - 1$.

Thus p cannot divide $x + y$, and by assumption $p \nmid a$. The rest of the proof parallels that of fermat's theorem, If we let x run from

$$a^h \prod x = \prod (ax) = \prod x^* \equiv (-1)^n \prod x$$

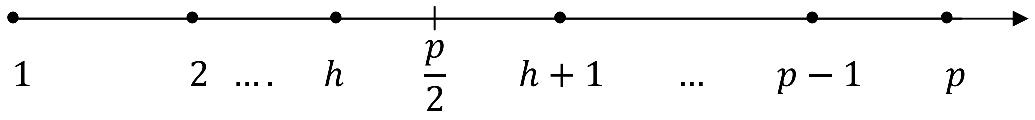
Cancelling $\prod x$ give $(-1)^n \equiv a^h$. But the latter is congruent to (a/p) by Euler is criterion.

The case $a -\ 2$.

We will use Gauss's lemma to compute (a/p) for some specific value of a. It is important to remember that we don't really need to odd or even.

(This is called the parity of n.)

Let us see what happens when $a\ = 2$. We are to find numbers x^* congruent to the number $2, 4\ , 5\ \dots ,2h = p - 1$ in the set$\{-h, -h + 1, \dots, h - 1, h\}$ and count how many of they are negative. (One example of how this works is given for $p = 13$ earlier in this section.) In general, n is the number of finger$x$ such that $p/2\ < 2\ x\ < p$, as the following picture shows .



Thus we must count the number of integer x such that p/4 < x < P/2. Of course, $p/4$ is not even an integer (nor is $p/2$), and so the smallest such $x$depends on what p is congruent to modulo 4. Let us suppose

$$p = 4\,q + r, \qquad o \leq \, r \, \leq 4$$

Since p is odd we must have $r \; = 1$ or 3. Then we must count the integers x such that $\frac{p}{4} = q + \frac{r}{4} < x < 2q + \frac{r}{2} = \frac{p}{2}$.

The first counted is clearly $q + 1$. And the last one counted is 2q or $2q + \; 1$, depending according as $r = \; 1$ or 3. The question is whether n is even or odd, which we see.

Depends on both the parity of a and whether r is 1 or 3. Let us check cases.

Case	$\boldsymbol{P = 4q + r}$	$\boldsymbol{n}$
$r = \; 1, q \; = \; 2s$	$8s + \; 1$	$q, even$
$r = 1, q = 2s + 1$	$8s \; + 5$	q, odd
$r = \; 3, q \; = \; 2s$	$8s \; + \; 3$	$q + 1, odd$
$r = 3, q = 2s + 1$	$8s \; + 7$	$q + 1, even$

Theorem (4.22):

Let P be an odd prime. Then $(2/P)$ is 1 if $P \; \equiv 1$ or 7 $(mod\; 8)$, and

$$\left(\frac{2}{p}\right) \text{is } -1 \text{ if} p \equiv \; 3 \; or \; 5 \; (mod \;\; 8)\,.$$

Example (4.23):

Compute (65/47):

Compute assign various parts of theorem and the result just proved we have .

$$\left(\frac{o\,5}{47}\right) = \left(\frac{18}{47}\right) = \left(\frac{2}{47}\right) = \left(\frac{9}{47}\right) = \left(\frac{2}{47}\right) = 1,$$

Where the last equality holds since 47 ≡ 7 (mod 8) the case a = 3

A similar argument to the one previously can be mode For a ≡ 2. Since we are assuming $p \nmid a$, then $p > \; 3$. The multiples of $1\,, 2, \ldots., h$ are $3, 6\,, 9, \ldots., 3\;h \; = \frac{3(p-1)}{2}$ all of which be between o and 3p/2. The following table shows what happens for p = $17 \; (\,s \; o \; h \; = \; 8)\,.$

x	1	2	3	4	5	6	7	8
$3x$	3	6	9	12	15	18	21	24
x^*	3	6	-8	-5	-2	1	4	7

The negative values of x^* correspond to $p/2 < x < p$ which is equivalent to $p/6 < x < p/3$.

The first integer after $p/6$ depends on the experience with $a = 2$ we will use the modulus 12 instead. Let $p = 12s + r, o \leq r \leq 12$.

Since neither 2 no r 3divide p, we must have $r = 1, 5, 7$ or 11 substituting $p = 12s + r$ into our inequality give

$$2s + \frac{r}{6} < x < 4s + \frac{r}{3} .$$

Since shifting either endpoint of a interval by an even integer does not change whether the number of integers in the interval is even or odd , it suffices to count the number of integers y satisfying $\frac{r}{6} < y < \frac{r}{3}$. The number of such y will be even or odd the same as n. we resort to cusses.

Case	Interval	Possible y	Parity of n
$r = 1$	$\frac{1}{6} < \mathrm{y} < \frac{1}{4}$	None	$Even$
$r = 5$	$\frac{5}{6} > y > 1\frac{2}{3}$	1	Odd
$r = 7$	$1\frac{1}{6} < \mathrm{y} < 2\frac{1}{3}$	2	Odd
$r = 11$	$1\frac{5}{6} > y > 3\frac{2}{3}$	2 , 3	$Even$

Theorem (4.24):

Let $p < 3$ be prime. Then $(3/p) = 1$ if $p = 1$ or 11 $(mod\ 12)$ and

$$(3/p) = -1 \text{ if } p = 5 \text{ or } 7\ (mod\ 12).$$

Quadratic Reciprocity:

The value of $(2/p)$ depends on what p is modulo 8. The value of $(3/p)$ depends on what $p$is Modulo 12.

Furthermore, some symmetry seems present. For example, $(2/\, p)$ has the same value has the same value whether $p \equiv 1(mod\ 8)\ or\ p \equiv -1 \equiv 7(mod\ 8)$and the same value whether

$$p \equiv 3\ (mod\ 8) \text{ or } p \equiv -3\ \equiv\ 5\ (mod\ \ 8).$$

The situation is similar for $a\ =\ 3$. Thus we might conjecture the following theorem.

Flipping a coin over the telephone:

Lemma (4.25):

Let $a\ >\ 0$, and let p and q be odd prime no dividing a. then $\left(\frac{a}{p}\right)\ =\ \left(\frac{a}{q}\right) if\ p =$ $q\ (mod\ 4\ a)$ or if $p\ =\ -q\ (mod\ 4a)$. The proof of this lemma which proceeds along lines similar to the cases $a = 2$ and $a = 3$ above, will be presented. For the time being, we will assume it is true and investigate its consequences. Suppose and a are distinct odd primes, so that each is congruent to either p nor q divider a. Then $p \equiv a(mod\ 4a)$ and so $(a/p) = (a/q)$ by lemma since

$q -\ p =\ 4a,$ the integer a has the interesting property that

$$q\ \equiv 4a\ (mod\ p) \text{and}\ p\ \equiv -4a\ (mod\ \ a)$$

Thus

$$\left(\frac{p}{q}\right) = \left(\frac{-4a}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{4}{q}\right)\left(\frac{a}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{4}{p}\right)\left(\frac{a}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{4a}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{p}{q}\right)$$

We have proved the following celebrated theorem.

Theorem (4.26):

Gausses law of quadratic reciprocity: suppose p and a are distinct odd primes, then $(p/q)\ =\ (q/p)$ unless p and q are both congruent to 3 module 4 in which case $(p/q)\ =\ -(q/p)$.

Example (4.27) :

Evaluate $(13/43)$ $(19/59)$ and $(37/67)$ since $13 \equiv 1(mod\ 4)$ we have

$$\left(\frac{13}{43}\right) = \left(\frac{43}{13}\right) = \left(\frac{3.13+4}{13}\right) = \left(\frac{4}{13}\right) =\ 1$$

where we used besides reciprocity, parts (4) and (1) of theorem likewise since both 19 and 59 are congruent to $3(\ mod\ 4)$ we have

$$\left(\frac{19}{59}\right) = -\left(\frac{59}{19}\right) = -\left(\frac{2}{19}\right) =\ 1$$

Since $(2/19) \; = \; -1$ by theorem. Finals since $37 \; \equiv \; 1 \; (mod \; 4)$

We have

$$\left(\frac{37}{67}\right) = \left(\frac{67}{37}\right) = \left(\frac{30}{37}\right) = \left(\frac{2}{37}\right)\left(\frac{3}{37}\right)\left(\frac{5}{37}\right)$$

$$= \; (-1)\left(\frac{37}{3}\right)\left(\frac{37}{3}\right) = - \; \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = -(1)(-1\;) = 1,$$

where theorem was used twice. Alternatively, we could not that

$$67 \; \equiv -7 \; (mod \; 37)$$

So

$$\left(\frac{67}{37}\right) = \left(\frac{-7}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{37}{7}\right) = (1)\left(\frac{2}{7}\right) = 1.$$

Flipping a can over the telephone the proof. Of lemma: our first order of business is to prove the lemma. Of the least section from which we derived the law of quadratic reciprocity.

Lemma (4.28):

Let $a > 0$ and let p and q be odd primes not dividing a. then $(a/p) = (a/q)$ if $p \equiv \; q(mod \; 4a)$.

Prove p. As with our evaluations of $(2/p)$ and $(3/p)$, we will employ gauss's lemma. Let $h \; = (\; p - 1)/2$, and consider the integers $a, 2a, 3a, \ldots.., ha$.

These fall into the open intervals $\left(0, \frac{p}{2}\right), \left(\frac{p}{2}, \frac{2p}{2}\right), \left(\frac{2p}{2}, \frac{3p}{2}\right), \; \left(\frac{3p}{2}, \frac{4p}{2}\right).$

Where a is customary,wear denoting the set of real numbers?

x. Such that $A < \; x < \; B$ by (A, B). since $ha = \frac{(p-1)a}{2} < \frac{pa}{2} < \frac{(p+1)a}{2} = (h+1)a$,The last interval we need consider is $(a-1)p/2, ap/2)$.

A total of a intervals are involved. So that the number of intervals does not depend on p.

Notice that the end points of the intervals listed iare either no integers or else multiples of p . Thus none of the integers $a, 2a, .., ha$ falls on one of these endpoints since $p \; x \; a$ and $h \; > \; p$.

$$\left(\frac{p}{2}, \frac{2p}{2}\right), \left(\frac{3p}{2}, \frac{4p}{2}\right), \left(\frac{5p}{2}, \frac{6p}{2}\right), \ldots \ldots..$$

Thus in a typical interval we want to count the number of integers x such that

$$\frac{(2k-1)p}{2} < \ ax < \frac{2kp}{2} \text{ . Or } \frac{(2k-1)p}{2a} < x < \frac{2kp}{2a}.$$

Now assume q is an odd frame such that q= $p \ (mod\ 4a)$.

Then $q \ = \ p + \ 4at$ for same integer . if we try to evaluate (a/q) by Gass's lemma in the same way, atypical interval in which we would be coming integers would be defined by the inequalities.

$\frac{(2k-1)a}{2a} < y < \frac{2ka}{2a}$ plugging $q \ = \ p + \ 4at$ into this leads to

$$\frac{(2k-1)p}{2a} + (2k-1)2\,t < y < \frac{2kp}{2a} + 4\,k\,t$$

(We leave it to the reader to cheek the algebra.

If we compare the endpoints of the intervals defined by the inequalities

we see that the left and points differ by even integers in the corresponding intervals differs try a multiple of 2, it is even in both cases or odd in both cases. Or odd in both cases.

By using the same argument for each value of k and applying Gauss's lemma we conclude that $(\ a/p) \ = \ (q/p)$.

Now we consider the case when q$\equiv -p \ (mod\ 4a)$. Then

$q = -p + 4at$ for some integer t. plugging this into (4.14) produces$\frac{-(2k-1)p}{2a} +$

$(2k-1)2t < y < \frac{-2kp}{2a} \ + 4\,k\,t$

Multiplying through by -1profuse a symmetric interval on the other side of 0 that contains the same number of integers,

$\frac{(2k-1)p}{2a} + 2t > y'' > \frac{2kp}{2a}$, In fact, the same number of integer are in the intervalshifred $4k\,f$ units to the right $- \frac{(2k-1)p}{2a} + \ (2k-1)\ 2 \ > y^{11} > \frac{2kp}{2a}$

Which can be written

$$\frac{2kp}{2a} < y'' < \frac{(2k-1)p}{2a} \ + \ 2\,t$$

We would like to show that the number of in foggersy^{11} satisfying these in equalities is even or odd the same as the number of x satisfying

define adjacent intervals, and the number of integers in their union is the number of 7 satisfying

$$\frac{(2k-1)p}{2a} < z < \frac{(2k-1)p}{2a} + 2\ t$$

(Recall that the endpoints of our interval are never hit so we need not worry about x equaling the common endpoint of the two intervals.)

The last inequalities define an interval of length $2t$ with no integral and points, It must contain an even number of integers, thus the number or of integers satisfying must be even in both eases or again using this argument for all values of k and applying Gauss's lemma we see that

$$\left(\frac{a}{q}\right) = (\frac{a}{p}).$$

References

1. Elementary number theory. University of new Hampshire, Editor in 1959.
2. Michio Suzuki,Group theory I, Berlin Heidelberg New York, Edition in 1977-1978.
3. Elements of the Representation theory if Associative Algebras – Ibrahim Assem and Andrzej skowronski, 2006.
4. Daniel Simson, London Mathematical Society's student text; 65.
5. Managing editor: professor J.W Bruce Department of Mathematics, University of Liverpool, UK.
6. Elementry Algebra, Daniel L.Auvil, Kent State University, edition published in 1984.