4. Basic Number Theory

Given any positive integer n and any integer a, if we divide a by n, we get a quotient q and a remainder r that obey the following relationship:

$$a = qn + r \qquad 0 \le r < n;\ q = [a/n]$$

where [x] is the largest integer less than or equal to x , the remainder r is often referred to as a **residue.** Example:

a=11;	n=7;	$11 = 1\times7+4$;	r =4
a=-11;	n=7;	$-11 = (-2)\times7+3$;	r =3

If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n. thus, for any integer a, we can always write

$$a = [a/n]\times n + (a \bmod n)$$

11 mod 7 =4; -11 mod 7 =3

Modular expression has the following laws:

Commutative laws	$(a+b) \bmod n = (b+a) \bmod n$
	$(a\times b) \bmod n = (b\times a) \bmod n$
Associative laws	$[(a+b)+c] \bmod n = [a+(b+c)] \bmod n$
	$[(a\times b)\times c] \bmod n = [a\times (b\times c)] \bmod n$
Distributive law	$[a\times(b\times c)] \bmod n = [(a\times b)(a\times c)] \bmod n$
Identities	$(0+a) \bmod n = a \bmod n$; $(1\times a) \bmod n = a \bmod n$

Two integers a and b are said to be **congruent modulo n** if (a mod n) = (b mod n). This is written $a \equiv b \bmod n$.

$73 \equiv 4 \bmod 23$; $21 \equiv -9 \bmod 10$

Note that if $a \equiv 0 \bmod n$, then $n \mid a$.

The congruent modulo operator has the following properties:

1. $a \equiv b \bmod n$ if $n \mid (a - b)$.
2. (a mod n) = (b mod n) implies $a \equiv b \bmod n$.
3. $a \equiv b \bmod n$ implies $b \equiv a \bmod n$.
4. $a \equiv b \bmod n$ and $b \equiv c \bmod n$.

To demonstrate the first point, if $n \mid (a-b)$ then $(a-b)=kn$ for some k. so we can write $a = b+kn$. Therefore, (a mod n)= (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) = (b mod n).

$23 \equiv 8 \pmod 5$	because	$23-8 = 15 = 5\times3$
$-11 \equiv 5 \pmod 8$	because	$-11-5 = -16 = 8\times-2$
$81 \equiv 0 \pmod{27}$	because	$81-0 = 81 = 27\times3$

Modular Arithmetic Operations

Modular arithmetic exhibits the following properties:

1. $[(a \bmod n) + (b \bmod n)] \bmod n = \mathbf{(a + b)} \bmod n$
2. $[(a \bmod n) - (b \bmod n)] \bmod n = \mathbf{(a - b)} \bmod n$
3. $[(a \bmod n) \times (b \bmod n)] \bmod n = \mathbf{(a \times b)} \bmod n$

The remaining properties are as easily proved. Here are examples of the three properties:

$11 \bmod 8 = 3$; $15 \bmod 8 = 7$
$[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$
$(11+15) \bmod 8 = 26 \bmod 8 = 2$
$[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$
$(11-15) \bmod 8 = -4 \bmod 8 = 4$
$[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$
$(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

Exponentiation is performed by repeated multiplication, as in ordinary arithmetic. (we have more to say about exponentiation)

To find $11^7 \bmod 13$, we can proceed as follows:
$11^2 = 121 \equiv 4 \bmod 13$
$11^4 \equiv 4^2 \equiv 3 \bmod 13$
$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \bmod 13$

Thus, the rules for ordinary arithmetic involving addition, subtraction, and multiplication carry over into modular arithmetic.

The following tables provide an illustration of modular addition and multiplication modulo 8. Looking at addition, the result are straightforward and there is a regular pattern to the matrix. Also, as in ordinary addition, there is an additive inverse, or negative, to each number in modular arithmetic. In this case, the negative of a number x is the number y such that $x + y \equiv 0 \bmod 8$. to find the additive inverse of a number in the left-hand column, scan across the corresponding row of the matrix to find the value 0; the number at the top of that column is the additive inverse; thus $2+6 = 0 \bmod 8$. similarly, the entries in the multiplication table are straightforward. In ordinary arithmetic, there is a multiplicative inverse, or reciprocal, to each number. In modular arithmetic mod 8, the multiplicative inverse of x is the number y such that $x \times y \equiv 1 \bmod 8$. now, to find the multiplicative inverse of a number from the multiplication table, scan across the matrix in the row for the that number to find the value 1; the number at the top of that column is the multiplicative; thus $3 \times 3 = 1 \bmod 8$. Note that not all numbers mod 8 have a multiplicative inverse; we will discuss this later.

Addition modulo 8

+ 0	1	2	3	4	5	6	7
0	1	2	3	4	5	6	7
1	2	3	4	5	6	7	0
2	3	4	5	6	7	0	1
3	4	5	6	7	0	1	2
4	5	6	7	0	1	2	3
5	6	7	0	1	2	3	4

6	7	0	1	2	3	4	5
7	0	1	2	3	4	5	6

Multiplication modulo 8

× 0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0
0	1	2	3	4	5	6	7
0	2	4	6	0	2	4	6
0	3	6	1	4	7	2	5
0	4	0	4	0	4	0	4
0	5	2	7	4	1	6	3
0	6	4	2	0	6	4	2
0	7	6	5	4	3	2	1

Additive and multiplicative inverses modulo 7

w	-w	w^{-1}
0	0	−
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

Modular Exponentiation

Throughout this book, we will be interested in numbers of the form

$$x^a \pmod{n} .$$

In this and the next coupe of sections, we discuss some properties of numbers raised to a power modulo an integer.

Suppose we want to compute 2^{1234} (mod 789). If we first compute 2^{1234}, then reduce mod 789, we'll be working with very large numbers, even though the final answer has only 3 digits. We should therefore perform each multiplication and then calculate the remainder. Calculating the consecutive powers of 2 would require that we perform the modular multiplication 1233 times. This method is too slow to be practical, especially when the exponent becomes very large. A more efficient way is the following (all congruences will be mod 789).

Suppose we want to compute 2^{1234} (mod 789). If we firt compute 2^{1234}, then reduce mod 789, we'll be working with very large numbers, even though the final answer has only 3 digits. We should therefore perform each multiplication and then calculate the remainder. Calculating the consecutive powers of 2 would require that we perform the modular multiplication 1233 times. This is method is too slow to be practical, especially when the exponent becomes very large. A more efficient way is the following (all congruences will be mod 789).

We start with $2^2 \equiv 4 \pmod{789}$ and repeatedly square both sides to obtain the following congruences:

$$\begin{array}{lllll}
2^4 & \equiv & 4^2 & \equiv & 16 \\
2^8 & \equiv & 16^2 & \equiv & 256 \\
2^{16} & \equiv & 256^2 & \equiv & 49 \\
2^{32} & \equiv & 34 & & \\
2^{64} & \equiv & 367 & & \\
2^{128} & \equiv & 559 & & \\
2^{256} & \equiv & 37 & & \\
2^{512} & \equiv & 580 & & \\
2^{1024} & \equiv & 286 & &
\end{array}$$

Since 1234 = 1024 + 128 + 64 +16 + 2 (this just means that 1234 equals 10011010010 in binary), we have

$$2^{1234} \equiv 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481 \pmod{789}$$

Basic Principles.

If gcd (a, n) = 1, then $1 \equiv a^{\Phi(n)} \pmod{n}$.

Note that when n = p is prime, Euler's theorem is the same as Fermat's theorem.

Let a, n, x, y be integers with $n \geq 1$ and gcd (a, n) = 1. ıf $x \equiv y \pmod{\Phi(n)}$, then $a^x \equiv a^y \pmod{n}$. In other words, if you want to work mod n, you should work mod Φ(n) in the exponent.

This extremely important fact will be used repeatedly in the remainder of the book. Review the preceding examples until you are conviced that the exponents mod 400 = Φ (100) and mod 100 are what count (i.e., don't be one of the many people who mistakenly try to work with the exponents mod 1000 and mod 101 in these examples).

Fermat's Little Theorem and Euler's Theorem

Two of the most basic results in number theory are Fermat's Little Theorems. Originally admired for their theoretical value, they have more recently proved to have important cryptographic applications.

Fermat's Little Theorem. If p is a prime and p does not divide a, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

example. $2^{10} = 1024 \equiv 1 \pmod{11}$. From this we can evaluate $2^{53} \pmod{11}$: write $2^{53} = (2^{10})^5 2^3 \equiv 1^5 2^3 \equiv 8 \pmod{11}$. Note that when working mod 11, we are essentially working with the exponents mod 10, not mod 11. In other words, from $53 \equiv 3 \pmod{10}$, we deduce $2^{53} \equiv 2^3 \pmod{11}$.

Usually, if $2^{n-1} \equiv 1 \pmod{n}$, the number n is prime. However, there are expections: $561 = 3 \cdot 11 \cdot 17$ is composite but $2^{560} \equiv 1 \pmod{561}$.we can conclude that $2^{560} \equiv 1 \pmod{11}$ and $2^{560} \equiv 1$

(mod 17).putting things together via the Chinese remainder theorem, we find that $2^{560} \equiv 1$ (mod 561).

Another such expection is $1729 = 7 \cdot 13 \cdot 19$. however, these exceptions are fairly rare in practice. Therefore, if $2^{n-1} \neq 1 (\text{mod } n)$, it is quite likely that n is prime. Of course, if $2^{n-1} \neq 1$ (mod n) then n cannot be prime. Since 2^{n-1} (mod n) can be evaluated very quickly, this gives a way to search for prime numbers. namely, choose a starting point n_0 and successively test each odd number $n \geq n_0$ to see whether $2^{n-1} \neq 1$ (mod n). ıf n fails the test, discard it and proceed to the next *n*. when an n passes the test, use more sophisticated techniques to test n for primality. The advantage is that this procedure is much faster than trying to factor each n, especially since it eliminates many n quickly. Of course, there are ways to speed up the search, for example, by first eliminating any n that has small prime factors.

We'll also need the analog of Fermant's theorem for a composite modulus n. Let $\Phi(n)$ be the number of integers $1 \leq a \leq n$ such that gcd (a, n) = 1. for example, if n= 10 then there are 4 such integers, namely 1,3,7,9. therefore, Φ (10) = 4. often Φ is called **Euler's Φ-function.**

Euler's Totient Function

Before presenting Euler's theorem, we need to introduce an important quantity in number theory, referred to as Euler's totient function and written Φ(n), where Φ(n) is the number of positive integers less than n and relatively prime to n.

It should be clear that for a prime number p,

$$\Phi(p) = p - 1$$

Now suppose that we have two prime numbers *p* and *q*. then, for n = *pq,*

$$\Phi(n) = \Phi(pq) = \Phi(p) \times \Phi(q) = (p-1) \times (q-1)$$

Same values of Euler's Totient Function Φ(n)

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

n	Φ(n)
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

n	Φ(n)
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

In particular, for prime p

Φ(p) = p-1

More generally, it can be deduced from the Chinese remainder theorem that for any integer n

$$\phi(n) = n\prod_{p|n}(1-\frac{1}{p}) \ ,$$

Where the product is over the distinct primes p dividing n. when n = *pq* is the product of two distinct primes, this yields

$$\Phi(pq) = (p\text{-}1)\ (q\text{-}1)$$

Examples.

Φ(10 = (2-1) (5-1) = 4,

Φ(120) = 120(1-1/2)(1-1/3)(1-1/5) = 32.

Example: what are the last there digits of 7^{803}?

Solution: Knowing the last three digits is the same as working mod 1000.
since *Φ*(1000) = 1000 (1-1/2) (1-1/5)= 400, we have $7^{803} = (7^{400})^2 7^3 \equiv 7^3 \equiv 343 \pmod{1000}$. Therefore, the last three digits are 343.

In this example, we were able to change the exponent 803 to 3 because 803 ≡ 3 (mod *Φ* (1000)).

Example: compute 2^{43210} (mod 101).
Solution: from Fermat's theorem, we know that $2^{100} \equiv 1$ (mod101). Therefore,

$$2^{43210} \equiv (2^{100})^{432}\, 2^{10} \equiv 1^{432}\, 2^{10} \equiv 1024 \equiv 14 \quad (\text{mod } 101).$$

In this case we were able to change the exponent 43210 to 10 because 43210 ≡ 10 (mod 100).

To summarize, we state the following:

Primitive Roots

Consider the powers of 3 (mod7):

$3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$.

Note that we obtain all the nonzero congruence classes mod 7 as powers of 3. This means that 3 is a primitive root mod 7 (the term *multiplicative generator* might be letter, but is not as common). The following summarizes the main facts we need about primitive roots.

Proposition. *Let g be a primitive root for the prime p.*

1. *if n is an integer, then $g^n \equiv 1$ (mod p) if and only if n ≡ 0 (mod p-1).*
2. *if j and k are integers, then $g^j \equiv g^k$ (mod p) if and only if j ≡ k (mod p-1).*

When p is prime, it is always possible to choose a so that a, a^2, a^3,……, a^{p-1} (all modula p) run through the values 1, 2, 3, ….., p-1 in some order. Such a is called a **generator** or a **primitive root of unity.** It turns out that out that for each prime p there is at least one generator. Indeed, the following theorem is true.

Recall *from* Euler's theorem that, for every a and n that are relatively prime,

$$a^{\Phi\,(n)} \equiv 1 \bmod n$$

Where $\Phi(n)$, Euler's totient function, is the number of positive integers less than n and relatively prime to n. Now consider the more general expression .

$$a^m \equiv 1 \bmod n$$

If a and n are relatively prime, then there is at least one integer m that satisfies Equation below namely, $m = \Phi(n)$. The least positive exponent m for which equation $a^m \equiv 1 \bmod n$ holds is referred to the exponent to which a belongs (mod n)

To see this last points consider the powers of 7, modulo 19:

$7^1 =$	7 mod 19
$7^2 = 49 = 2 \times 19 + 11 =$	11 mod 19
$7^3 = 343 = 18 \times 19 + 1 =$	1 mod 19
$7^4 = 2401 = 126 \times 19 + 7 =$	7 mod 19
$7^5 = 16807 = 884 \times 19 + 11 =$	11 mod 19

There is no point in continuing because the sequence is repeating. In other words, the sequence is periodic, and the length of the period is the smallest exponent m such that 7^m = 1(mod 19).

Table below shows all the powers of a modulo 19 for all positive a .

The length of the sequence for each base value is indicated by shading. Note the following:

1- All sequences end in 1. This is consistent with the reasoning of the preceding few paragraphs.
2- The length of sequence divides Φ(19) = 18. That is, an integral number of sequences occur in each row of the table.
3- Some of the sequences are of length 18. In this case, it is said that the base integer a generates (via powers) the set of nonzero integers modulo 19.
   Each such integer is called a primitive root of the modulus 19.

Table 7.6 powers of integers, modulo 19

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

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

In general, when p is a prime, a primitive root mod p is a number whose powers yield every nonzero and non repeated class mod p. there are Φ(p-1) primitive roots mod p. In particular, there is always at least one.

In practice, it is not difficult to find one, at least if the factorization of p-1 is known.

The importance of this notion is that if *a* is a primitive root of *n,* _, then its powers

$$a, a^2, \ldots, a^{\Phi(n)}$$

are distinct (mod *n)* and are all relatively prime to *n.* In particular, for a prime number *p*,if a is a primitive root of *p*, then

$$a, a^2, \ldots\ldots a^{p-1}$$

are distinct *(modp).* For the prime number 19, its primitive roots are 2, 3, 10, 13,14,and 15

Not all integers have primitive roots. In fact, the only integers with primitive roots are those of the form2, 4, p^{α} and $2p^{\alpha}$, where *p* is any odd prime.

More generally, we can say that the highest possible exponent to which a number can belong (mod *n*) is Φ (*n*). If a number of this order, it is referred to as a primitive root of n. the importance of this notion is that if a is a primitive root of n, then its powers

$$a, a^2, \ldots\ldots, a^{\Phi(n)}$$

are distinct (mod *n*) and are all relatively prime to *n*. In particular, for a prime number *p*, if a is a primate root of *p*, then

$$a, a^2, \ldots.., a^{p-1}$$

are distinct (mod *p*). for the prime number 19, its primitive roots are 2, 3, 10, 13, 14, and 15.

Not all integers have primitive roots. In fact, the only integers with primitive root are those of the form 2, 4, p^{α}, and $2p^{\alpha}$, where p is any odd prime.

The Chinese Remainder Theorem

In many situations, it is useful to break a congruence mod n into a system of congruencies mod factors of n. Consider the following example. Suppose we know that a number x satisfies x ≡ 25 (mod 42). This means that we can write x = 25 + 42*k* for some integer k. rewriting 42 as 7· 6, we obtain x = 25 + 7 (6k), which implies that x ≡ 25 ≡ 4 (mod 7). Similarly, since x = 25 + 6(7k), we have x ≡ 25 1 (mod 6). Therefore,

$$x \equiv 25 \pmod{42} \rightarrow \begin{cases} x \equiv 4 & (\text{mod}\,7) \\ x \equiv 1 & (\text{mod}\,6). \end{cases}$$

the Chinese remainder theorem shows that a system of congruences can be replaced by a single congruence under certain conditions.

Theorem. *Suppose* gcd *(m, n) = 1. given a and b, there exist exactly one solution x (*mod *mn) to the simultaneous congruence under certain conditions.*

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}.$$

Proof. There exist integers *s, t* such that $ms + nt = 1$. then $ms \equiv 1 \pmod{n}$ and $nt \equiv 1 \pmod{m}$. Let $x = bms + ant$. Then $x \equiv ant \equiv a \pmod{m}$, and $x \equiv bms \equiv b \pmod{n}$, as desired. Suppose x_1 is another solution. Then $x \equiv x_1 \pmod{m}$ and $x \equiv x_1 \pmod{n}$, so $x-x_1$ is a multiple of both m and n.

Lemma. Let *m, nbe integers with* gcd *(m,n) = 1. If an integer c is a multiple of both m and n, then c is a multiple of mn.*

Proof. Let $c = mk = nl$. Write $ms + nt = 1$ with integers *s, t.* multiply by *c* to obtain $c = cms + cnt = mnls + mnkt = mn\,(ls + kt)$.

To finish the proof of the theorem, let $c = x - x_1$ in the lemma to find that $x - x_1$ is a multiple of *mn.* Therefore, $x \equiv x_1 \pmod{mn}$. This means that any two solutions x to the system of congruences are congruent mod *mn,* as claimed.

Example: solve $x \equiv 3 \pmod{7}$, $x \equiv 5 \pmod{15}$.
Solution : $x \equiv 80 \pmod{105}$ (note: $105 = 7 \cdot 15$). Since $80 \equiv 3 \pmod{7}$ and $80 \equiv 5 \pmod{15}$, 80 is a solution. The theorem guarantees that such a solution exists, and says that it is uniquely determined mod the product *mn*, which is 105 in the present example.

How does one find the solution? One way, which works with small numbers m and *n*, is to list the numbers congruent to b (mod *n*) until you find one that is congruent to a (mod *m*). for example, the numbers congruent to 5 (mod 15) are

5, 20, 35, 50, 65, 80, 95, …..

Mod 7, these are 5, 6, 0, 1, 2, 3, 4, …… since we want 3 (mod 7), we choose 80.

For slightly larger numbers m and n, making a list would be inefficient. However, a similar idea works. The numbers congruent to b (mod n) are of the form $b + nk$ with k an integer, so we need to solve $b + nk \equiv a \pmod{m}$. this is the same as

$$nk \equiv a - b \pmod{m}.$$

since $\gcd(m, n) = 1$ by assumption, there is a multiplicative inverse *i* for *n* (mod *m*). multiplication by I gives

$$k \equiv (a - b)i \pmod{m}.$$

substituting back into $x = b + nk$, then reducing mod mn, gives the answer.

Of course, for large numbers, the proof of the theorem gives an efficient method for finding x that is almost the same as the one just given.

Example: solve $x \equiv 7 \pmod{12345}$, $x \equiv 3 \pmod{11111}$.
Solution: first, we know from our calculations in section that the inverse of 11111 (mod 12345) is i = 2471. therefore $k \equiv 2471\,(7 - 3) \equiv 9884 \pmod{12345}$.this yields $x = 3 + 11111 \equiv 9884 \equiv 109821127 \pmod{(11111 \cdot 12345)}$.

How do you use the Chinese remainder theorem? The main idea is that if you start with a congruence mod a composite number n, you can break it into simultaneous congruences mod each prime power factor of n, then recombine the resulting information to obtain an answer mod n. the advantage is that often it is easier to analyze congruences mod primes or mod prime powers than to work mod composite numbers.

Suppose you want to solve $x^2 \equiv 1 \pmod{35}$. Note that $35 = 5 \cdot 7$. we have

$$x^2 \equiv 1 \pmod{35} \leftrightarrow \begin{cases} x^2 \equiv 1 \pmod{7} \\ x^2 \equiv 1 \pmod{5}. \end{cases}$$

now, $x^2 \equiv 1 \pmod{5}$ has 2 solutions: $x \equiv \pm 1 \pmod{5}$. Also, $x^2 \equiv 1 \pmod{7}$ has 2 solutions: $x \equiv \pm 1 \pmod{7}$. We can put these together in 4 ways:

$x \equiv 1 \pmod{5}$, $x \equiv 1 \pmod{7}$ → $x \equiv 1 \pmod{35}$,

$x \equiv 1 \pmod{5}$, $x \equiv -1 \pmod{7}$ → $x \equiv 6 \pmod{35}$,

$x \equiv -1 \pmod{5}$, $x \equiv 1 \pmod{7}$ → $x \equiv 29 \pmod{35}$,

$x \equiv -1 \pmod{5}$, $x \equiv -1 \pmod{7}$ → $x \equiv 34 \pmod{35}$.

So the solutions of $x^2 \equiv 1 \pmod{35}$ are $x \equiv 1, 6, 29, 34 \pmod{35}$.

In general, if $n = p_1p_2 \dots p_r$ is the product of r distinct odd primes, then $x^2 \equiv 1 \pmod{n}$ has 2^r solutions. This is a consequence of the following.

Chinese Remainder Theorem (General Form).

Let $m_1, \dots, m_k$ be integers with gcd $(m_i, m_j) = 1$ whenever $i \neq j$. given integers $a_1, \dots, a_k$, there exists exactly one solution x (mod $m_1 \dots m_k$) to the simultaneous congruences

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}, \dots, x \equiv a_k \pmod{m_k}$.

for example, the theorem guarantees a solution to the simultaneous congruences

$x \equiv 1 \pmod{11}$, $x \equiv -1 \pmod{13}$, $x \equiv 1 \pmod{17}$.

In fact, $x \equiv 1871 \pmod{11 \cdot 13 \cdot 17}$ is the answer.

For a procedure that produces the number x in the theorem.

Square Roots Mod n

Suppose we are told that $x^2 \equiv 71 \pmod{77}$ has a solution. How do we find one solution, and how do we find all solutions? More generally, consider the problem of finding all solutions of $x^2 \equiv b \pmod{n}$, where n=pq is the product of two primes. We show in the following that this can be done quite easily, once the factorization of n is known. Conversely, if we know all solutions, then it is easy to factor n.

Let's start with the case of square roots mod a prime p. The easiest case is when $p \equiv 3 \pmod{4}$, and this suffices for our purposes. The case when $p \equiv 1 \pmod{4}$ is more difficult.

Proposition.

Let $p \equiv 3 \pmod{4}$ be prime and let y be an integer. Let $x \equiv y^{(p+1)/4} \pmod{p}$.

1. If y has a square root mod p, then the square roots of y mod p are $\pm$.

2. If y has no square root mod p, then –y has a square root mod p, and the square roots of –y are $\pm$.

Proof. If $y \equiv 0 (\bmod p)$, all the statements are trivial, so assume $y \neq 0$ (mod p).Fermat's theorem says that $y^{p-1} \equiv 1 (\bmod p)$. Therefore,

$$x^4 \equiv y^{p+1} \equiv y^2 y^{p-1} \equiv y^2 (\bmod p).$$

This implies that $(x^2 + y)(x^2 - y) \equiv 0 (\bmod p)$, so $x^2 \equiv \pm y (\bmod p)$. Therefore, at least one of y and –y is a square mod p. Suppose both y and –y are squares mod p, say $y \equiv a^2$ and $-y \equiv b^2$. Then $-1 \equiv (a/b)^2$ (work with fractions mod p as in Section 3.3), which means -1 is a square mod p. This is impossible when $p \equiv 3 (\bmod 4)$ (see Exercise 15). Therefore, exactly one of y and –y has a square root nod p. If y has a square root mod p then $y \equiv x^2, and$ the two square roots of y are $\pm$. If –y has a square root then $x^2 \equiv -y$.

Example. Let's find the square root of 5mod11. Since (p+1)/4=3, we compute $x \equiv 5^3 \equiv 4 (\bmod 11)$ .Since $4^2 \equiv 5 (\bmod 11)$, the square roots of 5 mod 11 are ± 4.

Now let's try to find a square root of 2 mod 11.Since (p+1)/4=3, we compute $2^3 \equiv 8 (\bmod 11)$. But $8^2 \equiv 9 \equiv -2 (\bmod 11)$, so we have found a square root of -2 rather than of 2.This is because 2 has n square root mod 11.

We now consider square roots a composite modulus. Note that

$x^2 \equiv 71 (\bmod 77)$ means that

$x \equiv \pm 1 (\bmod 7)$ and $x \equiv \pm 4 (\bmod 11)$.

The Chinese remainder theorem tells us that a congruence mod 7 and a congruence mod 11 can be combined into a congruence mod 77. For example, if $x \equiv 1 (\bmod 7)$ and $x \equiv 4 (\bmod 11)$, then $x \equiv 15 (\bmod 77)$. In this way, we can combine in four ways to get the solutions

$$x \equiv \pm 15, \ \pm 29 (\bmod 77).$$

Now let's turn things around. Suppose n=pq is the product of two primes and we know the four solutions $x \equiv \pm a, \ \pm b$ of $x^2 \equiv y (\bmod n)$.

Finding the Greatest Common Divisor

One of the basic techniques of number theory is Euclid's algorithm, which is a simple procedure for determining the greatest common divisor of two positive integers. An extended form of Euclid's algorithm determines the greatest common divisor of two positive integers and, if those numbers are relatively prime, the multiplicative inverse of one with respect to the other.

Euclid's algorithm is based on the following theorem: For any nonnegative integer *a* and any positive integer *b*,

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

$$\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11)$$

to see this, consider if d = gcd (*a, b*). Then, by the definition of gdc, $d \mid a$ and $d \mid b$. for any positive integer *b, a* can be expressed in the form

a = kb + r ≡ r mod b
a mod b = r

therefore, (a mod b) = $a - kb$ for some integer k. But because $d \mid b$, it also divides kb. We also have $d \mid a$. therefore, $d \mid (a \text{ mod } b)$. This shows that d is a common divisor of b and (a mod b). conversely, if d is a common divisor of b and (a mod b), then $d \mid kb$ and thus $d \mid [kb + (a \text{ mod } b)]$, which is equivalent to $d \mid a$. Thus, the set of common divisors of a and b is equal to the set of common divisors of b and (a mod b). Therefore the gcd of one is the same as the gcd of the other, proving the theorem.

Equation can be used repetitively to determine the greatest common divisor.

gcd (18,12) = gcd (12, 6) = gcd (6, 0) = 6
gcd (11,10) = gcd (10, 1) = gcd (1, 0) = 1

Euclid's algorithm makes repeated use of equation to determine the greatest common divisor, as follows. The algorithm assume $d>f > 0$. It is acceptable to restrict algorithm to positive integers because gcd (a, b) = gcd ($|a|, |b|$).

To find the gcd (1970, 1066),	
1970 = 1×1066+904	gcd(1066, 904)
1066 = 1×904+162	gcd(904,162)
904 = 5×162+94	gcd(162, 94)
162 = 1×94+68	gcd(94, 68)
94 = 1×68+26	gcd(68, 26)
68 = 2×26+16	gcd(26, 16)
26 = 1×16+10	gcd(16, 10)
16 = 1×10+6	gcd(10, 6)
10 = 1×6+4	gcd (6, 4)
6 = 2×2+2	gcd(4, 2)
2 = 2×2+0	gcd(2, 0)
Therefore, gcd (1970, 1066) = 2.	

The alert reader may ask how we can be sure that this process terminates. That is, how can we be sure that at some point Y divides X? ıf not, we would get an endless sequence of positive integers, each one strictly smaller than the one before, and this is clearly impossible.