Computational Number Theory and Public Key Cryptography (INF 245), fall 2020

Igor Semaev

September 14, 2022

1 Chapter 2. Introduction to Number Theory.

1.1 Arithmetic of integers. Euclidean algorithm.

Let a, b be integers and $a \neq 0$. One says a divides b if there exists an integer k such that $b = ak$. This is denoted by $a|b$. One also says b is a multiple of a.

Proposition 1. *1. For every $a \neq 0$, $a|0$, and $a|a$, and $1|b$ for every b.*

2. If $a|b$ and $b|c$ then $a|c$.

3. If $d|a$ and $d|b$ then $d|ax + by$ for all integers x, y

The greatest common divisor of integer a, b is the largest positive integer c such that $c|a$ and $c|b$. Notation $c = \gcd(a, b)$. We say a, b are relatively prime(coprime) if $\gcd(a, b) = 1$

Theorem 1. *Let $a \neq 0$ and b be integers. Then there exist two unique integers q and r such that $b = aq + r$ and $0 \leq r < |a|$.*

Proof. First we show that q, r exist. Let c be the greatest integer $\leq b/|a|$. Then $b/|a| = c + \alpha$, where $0 \leq \alpha < 1$. We have $b = |a|(c + \alpha) = c|a| + \alpha|a|$. We put $r = \alpha|a|$, that is an integer number and $0 \leq r < |a|$. Let $q = c$ if a positive and $q = -c$ if a negative. Then $b = qa + r$ as stated.

Now we show that q and r are unique. If not, then $b = q_1 a + r_1$, for other q_1, r_1 and $0 \leq r_1 < |a|$. Then

$$|q - q_1| = |r - r_1|/|a| < 1.$$

So $q = q_1$ and therefore $r = r_1$. □

Theorem 2. *Let $b = qa + r$. Then $\gcd(b, a) = \gcd(a, r)$.*

Proof. Let $d = \gcd(b, a)$ and $e = \gcd(a, r)$. Then $d|r = b - qa$ and therefore $d|e$. Also $e|b$ and therefore $e|d$. One concludes $d = e$. □

We explain a simple form of the Euclidean algorithm. Let $a_0 = a, a_1 = b$, where $a \geq b > 0$. One applies the division algorithm (Theorem 1) iteratively and get

$$a_i = q_{i+1}a_{i+1} + a_{i+2}, \text{where} \quad 0 < a_{i+2} < a_{i+1}$$

for $0 \leq i < n-1$ and $a_{n+1} = 0$ for some n.

Theorem 3. *The algorithm terminates and* $\gcd(a, b) = a_n$.

Proof. The algorithm will terminate as $a_0 \geq a_1 > a_2 > \ldots \geq 0$ and at some point the remainder is zero. By Theorem 2,

$$\gcd(a, b) = \gcd(a_0, a_1) = \ldots = \gcd(a_{n-1}, a_n) = \gcd(a_n, 0) = a_n.$$

Therefore, $\gcd(a, b) = a_n$. □

Theorem 4. *Let* $d = \gcd(a, b)$*, then* a/d *and* b/d *are coprime.*

Proof. If a/d and b/d are not coprime, then some $s > 1$ is their common divisor. Therefore, $ds|a$ and $ds|b$. As $ds > d$ this contradicts d is the gcd of a, b. □

Theorem 5. *If* a, b *are not both zero, then there are integer* x, y *such that* $ax + by = \gcd(a, b)$.

Proof. Let g be the smallest positive integer such that $g = ax + by$. It obviously exists. By Proposition 1, $\gcd(a, b)|g$. Let's prove that $g|a$. If not then $a = qg + r$, where $0 < r < g$. Then $r = a - qg = a - q(ax + by) = a(1 - qx) + b(-qy)$. That contradics the fact that g is the smallest positive integer of the form $ax + by$. Hence, $g|a$. Similarly, $g|b$ and so $g|\gcd(a, b)$. Therefore, $g = \gcd(a, b)$. □

For $a \geq b > 0$ the following Extended Euclidean Algorithm finds integers x, y such that $ax + by = \gcd(a, b)$.

1. Initialize $A_1 = (1, 0, a), A_2 = (0, 1, b)$.
2. While $A_2[3] > 0$ do
   (a) $q = \lfloor A_1[3]/A_2[3] \rfloor$,
   (b) $B = A_1 - qA_2, A_1 = A_2, A_2 = B$.
3. Terminate with $A_1 = (x, y, \gcd(a, b))$.

Obviously, the algorithm implements ordinary Euclidean algorithm for $A_1[3], A_2[3]$. As $aA_i[1] + bA_i[2] = A_i[3]$ initially, that holds at each step. After terminating $A_1[3] = \gcd(a, b)$. So the algorithm really solves the problem.

1.2 Prime Numbers

A prime number is an integer $p > 1$ divisible only by 1 and itself, and by no other positive integers. A composite number is an integer $n > 1$ which is not prime. A composite number has a positive divisor other than 1 and itself.

Lemma 1. *Let a, b, c be integers. If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.*

Proof. As a, b are coprime, by Theorem 5 there are integers x, y such that $ax + by = \gcd(a, b) = 1$. Hence $axc + byc = c$. As $a|axc$ and $a|bcy$, we have $a|c$ as stated. □

Lemma 2. *If a prime number p divides a product $a_1 \dots a_n$ of integers, then p divides at least one of them.*

Proof. We will prove the lemma by induction on n. If $n = 1$, then nothing is to prove. Assume the statement is true for $n \geq 1$ factors. Let's prove it for $n + 1$ factors. Let $p|a_1 \dots a_n a_{n+1}$. If $p|a_{n+1}$, then we are done. Otherwise p and a_{n+1} are coprime. In that case, by Lemma 1, $p|a_1 \dots a_n$ and p divides at least one of $a_1, \dots, a_n$ by induction. □

Theorem 6. *Every integer $n > 1$ may be written as a product of powers of different primes*

$$n = p_1^{e_1} \dots p_s^{e_s},$$

where $e_1, \dots, e_s \geq 1$. This presentation is unique.

Proof. If $n > 1$ is the least integer which is not a product of prime numbers. Then n has to be composite and one writes $n = ab$, where $1 < a < n$ and $1 < b < n$. Since $a, b < n$, one writes them as the product of primes. Then $n = ab$ may be written as the product of primes. Therefore every $n > 1$ may be written as the product of powers of primes.

We now show that this product is unique up to the order of the primes in the product. Assume that is not, then

$$n = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l, \tag{1}$$

where $p_1, p_2, \dots, p_k$ and $q_1, q_2, \dots, q_l$ are not necessarily different prime numbers. As q_1 divides the product $p_1 p_2 \dots p_k$, it divides at least one of the primes $p_1, p_2, \dots, p_k$ by Lemma 2. We may assume $q_1|p_1$ and therefore $q_1 = p_1$. We divide the both sides of (1) by q_1, get

$$p_2 \dots p_k = q_2 \dots q_l$$

and repeat the argument to prove the presentation is unique. □

Let $p_1, p_2, \dots, p_k$ be primes that divide either of the positive integers m and n. We can write

$$n = p_1^{e_1} \dots p_k^{e_k}, \quad m = p_1^{f_1} \dots p_k^{f_k},$$

where $e_i, f_i \geq 0$. The following statement is obvious.

Theorem 7.

$$\begin{aligned} \gcd(n,m) &= p_1^{\min(e_1,f_1)} \dots p_k^{\min(e_k,f_k)}, \\ lcm(n,m) &= p_1^{\max(e_1,f_1)} \dots p_k^{\max(e_k,f_k)}. \end{aligned}$$

The least common multiple of positive integers n, m is the smallest positive integer divisible by n and m. It is denoted $\mathrm{lcm}(n,m)$. The theorem implies $\gcd(n,m)\,\mathrm{lcm}(n,m) = nm$.

Theorem 8. *The number of primes is infinite.*

Proof. Let $p_1, \dots, p_k$ be all primes and $n = p_1 \dots p_k + 1$. By Theorem 6 there is a prime $p|n$. Therefore, p is one of $p_1, \dots, p_k$, say $p = p_1$. Hence $p|n - p_1 \dots p_k = 1$. That is a contradiction. So the number of primes is infinite. □

One can prove that the gap between two consecutive prime numbers may be larger than any given natural number. However there are consecutive primes whose difference is 2, they are called twin primes. For instance, 3 and 5, 17 and 19, 101 and 103, 3671 and 3673.

A prime p for which $2p + 1$ is prime is called a Sophie Germain prime. The first Sophie Germain primes are 2,3,5,11,23,29,41,53. It was conjectured that the set of twin and Sophie Germain primes are infinite.

For a real $x > 0$ let $\pi(x)$ denote the number of primes $p \le x$.

Theorem 9. *(Prime Number Theorem)* $\lim_{x\to\infty} \frac{\pi(x)}{x/ln\,x} = 1$.

The proof of this theorem is out of the cryptography course scope. The probability that a random $1 \le n \le x$ is a prime number is obviously $\frac{\pi(x)}{x}$. The theorem implies that this probability is $\approx \frac{1}{ln\,x}$ for large x.

Theorem 10. *Let $n > 1$ be composite, then it has a prime factor $p \le \sqrt{n}$.*

Proof. As n is composite, then $n = ab$, where $a > 1$ and $b > 1$. At least one of a, b is $\le \sqrt{n}$. Otherwise, if $a, b > \sqrt{n}$ both, then $ab > \sqrt{n}\sqrt{n} = n$. This is a contradiction. So let $a \le \sqrt{n}$. Let p be a prime factor of a. So $p|n$ and $p \le \sqrt{n}$. □

The theorem implies that if an integer $n > 1$ has no prime factors $p \le \sqrt{n}$, then n is prime. In order to test n for primality, one runs over primes $p \le \sqrt{n}$ and checks if $p|n$. If not for all such primes then n is prime itself. In practice, it is better (it is not necessary to generate those primes) to run over all natural $d \le \sqrt{n}$ and check if $d|n$. The number of trial divisions is at most $\sqrt{n}$.

One can use Theorem 10 to construct all the primes up to some limit n by crossing out composite numbers. The algorithm is called Eratosthenes sieve.

1. Write all the integers between 2 and n in a list. Let $p = 2$.
2. Cross out all numbers in the list multiple to p except p. Let $p \le \sqrt{n}$ be the next uncrossed number in the list. Repeat the step. Otherwise, if there are no uncrossed $p \le \sqrt{n}$, terminate.

For each prime $p \leq \sqrt{n}$ one crosses out at most $\lfloor n/p \rfloor$ numbers. Overall complexity is at most (we sum over all integers $k \leq \sqrt{n}$ below)

$$\sum_{k=2}^{\sqrt{n}} \lfloor n/k \rfloor \approx n \int_2^{\sqrt{n}} \frac{dx}{x} = n\,ln\sqrt{n} - n\,ln2 = O(n \ \ln \ n)$$

steps. In fact, the number of operations is at most $O(n \ \ln\ln \ n)$, since

$$\sum_{p=2}^{\sqrt{n}} 1/p \approx \ln\ln n,$$

where we sum over only primes.

Testing all integers between 2 and n with trial divisions would take around $n\sqrt{n} = n^{3/2}$ divisions. So the Eratosthenes sieve is more efficient though it requires storage of the same order of magnitude as the number of steps. Later we will study more efficient methods for testing and constructing large prime numbers.

1.3 Congruences

Let a, b be integers and $m > 1$ be a positive integer. We say a is congruent to b modulo m if m divides $a - b$. We then write $a \equiv b (\mathrm{mod}\, m)$ and call the formula a congruence. Obviously, $a \equiv b (\mathrm{mod}\, m)$ if and only if $a = b + km$ for an integer k. If $d|m$, then $a \equiv b (\mathrm{mod}\, m)$ implies $a \equiv b (\mathrm{mod}\, d)$. The congruence is a equivalence relation according to the following statement.

Theorem 11. *Let m be a positive integer and a, b, c be any integers. Then*

1. $a \equiv a (mod\, m)$.
2. *If* $a \equiv b (mod\, m)$, *then* $b \equiv a (mod\, m)$
3. *If* $a \equiv b (mod\, m)$ *and* $b \equiv c (mod\, m)$, *then* $a \equiv c (mod\, m)$

For each integer a the set of integers $b \equiv a (\mathrm{mod}\, m)$ is called residue class of a modulo m and a is called a residue of b and b is called a residue of a. Each residue class contains exactly one integer from $0, 1, \ldots, m-1$. That follows from the division with remainder. For any a we can write $a = qm + r$, where $0 \leq r \leq m - 1$ and $a \equiv r (\mathrm{mod}\, m)$.

Theorem 12. *Let m be a positive integer and a, b, c, d be any integers. Suppose* $a \equiv b (mod\, m)$ *and* $c \equiv d (mod\, m)$. *Then* $a \pm c \equiv b \pm d (mod\, m)$ *and* $ac \equiv bd (mod\, m)$.

Proof. By assumption, $a = b + km$ and $c = d + lm$ for some integer k, l. So $a \pm c = (b + km) \pm (d + lm) = b \pm d + (k \pm l)m$ and therefore $a \pm c \equiv (b \pm d) (\mathrm{mod}\, m)$. Similarly, $ac = (b + km)(d + lm) = bd + (bl + kd + klm)m$ implies $ac \equiv bd (\mathrm{mod}\, m)$. □

Corollary 1. *Let a, b be integers and $f(x)$ be a polynomial with integer coefficients. If $a \equiv b (mod\, m)$, then $f(a) \equiv f(b) (mod\, m)$.*

Theorem 13. *If $\gcd(a, m) = 1$, then there is an integer x such that $ax \equiv 1 (mod\, m)$. Let b, c be integers, then $ab \equiv ac (mod\, m)$ implies $b \equiv c (mod\, m)$.*

Proof. Theorem 5 implies that $ax + my = \gcd(a, m) = 1$ for some integer x, y. Hence, $ax \equiv 1 (\mathrm{mod}\, m)$ and the first statement is proved. The congruence $ab \equiv ac (\mathrm{mod}\, m)$ implies $xab \equiv xac (\mathrm{mod}\, m)$. So $b \equiv c (\mathrm{mod}\, m)$. □

1.4 Linear Congruences

We study how to find an integer (a residue) x such that $ax \equiv b (\mathrm{mod}\, m)$. The latter is called a linear congruence. For instance, the solution to the congruence $2x \equiv 1 (\mathrm{mod}\, 5)$ is $x = 5k + 3$ for any integer k.

Theorem 14. *The congruence $ax \equiv b (mod\, m)$ has a solution if and only if $\gcd(a, m) | b$.*

Proof. The congruence $ax \equiv b (\mathrm{mod}\, m)$ is equivalent to $ax = b + mk$ for some integer k. Let $g = \gcd(a, m)$. If the congruence has a solution then $g | ax - mk = b$ and the statement is proved in one direction. Assume now $g | b$. One divides both sides of $ax = b + mk$ by g and gets $a_1 x = b_1 + m_1 k$, where $a_1 = a/g, b_1 = b/g, m_1 = m/g$. By the definition of $g = \gcd(a, m)$, the numbers a_1, m_1 are coprime, and so a_1 is invertible modulo m_1. Therefore the congruence $a_1 x = b_1 (\mathrm{mod}\, m_1)$ has a solution. The solution x is a solution for the initial congruence $ax \equiv b (\mathrm{mod}\, m)$ as well. □

The theorem gives a method of computing a solution if the theorem assumptions are fulfilled. It is based on inverting modulo $m/\gcd(a, m)$.

Corollary 2. *Let $g = \gcd(a, m) | b$, then the congruence $ax \equiv b (mod\, m)$ has exactly g solutions. If x_0 is one of the solutions then all other solutions are $x_0 + (m/g)t\, (mod\, m)$ for $0 \leq t \leq g - 1$.*

Proof. Let x_0 be a solution, then $x = x_0 + (m/g)t\, (\mathrm{mod}\, m)$ for $0 \leq t \leq g - 1$ are different residues modulo m and the solutions too. That is true because

$$ax = a(x_0 + (m/g)t) = ax_0 + (am/g)t = ax_0 + (a/g)mt \equiv b (\mathrm{mod}\, m)$$

and a/g is an integer number.

Let's prove that those are all solutions. Let $ax_1 \equiv b (\mathrm{mod}\, m)$, then one subtracts this congruence from $ax_0 \equiv b (\mathrm{mod}\, m)$ and gets $a(x_0 - x_1) \equiv 0 (\mathrm{mod}\, m)$. The latter is equivalent to $m | a(x_1 - x_0)$. Therefore, $(m/g) | (a/g)(x_1 - x_0)$. As $\gcd(m/g, a/g) = 1$ we get, by Lemma 1, that $(m/g) | (x_1 - x_0)$. So $x_1 = x_0 + (m/g)t$ for some integer t. Instead of t one takes its residue modulo g within $0, 1, \ldots, g - 1$. □

1.5 The Chinese Remainder Theorem

Theorem 15. *Let $n_1, \ldots, n_r$ be r positive pairwise coprime integers. Let $a_1, \ldots, a_r$ be any r integers. There is exactly one residue (residue class) a modulo $n = n_1 \ldots n_r$ such that*

$$a \equiv a_i \,(mod\, n_i), \quad i = 1, \ldots, r. \tag{2}$$

Proof. We will prove the statement for $r = 2$ first. As n_1, n_2 are coprime, there are integers x, y such that $xn_1 + yn_2 = 1$. So $xn_1 \equiv 1 (\mathrm{mod}\, n_2)$ and $yn_2 \equiv 1 (\mathrm{mod}\, n_1)$. Let $a = xn_1a_2 + yn_2a_1$, then $a \equiv yn_2a_1 \equiv a_1 (\mathrm{mod}\, n_1)$ and $a \equiv xn_1a_2 \equiv a_2 (\mathrm{mod}\, n_2)$. Therefore a is a solution to (2).

Let $r > 2$. We can use induction. By induction, there is a residue a' modulo $n' = n_1 \ldots n_{r-1}$ such that $a' \equiv a_i \,(\mathrm{mod}\, n_i), \quad i = 1, \ldots, r-1$. The numbers n', n_r are coprime. Therefore there is a residue a modulo $n = n'n_r$ such that $a \equiv a' \,(\mathrm{mod}\, n')$ and $a \equiv a_r \,(\mathrm{mod}\, n_r)$. That is a solution to (2).

Assume another solution b. By subtracting $a \equiv a_i \,(\mathrm{mod}\, n_i)$ and $b \equiv a_i \,(\mathrm{mod}\, n_i)$, one gets $a - b \equiv 0 (\mathrm{mod}\, n_i)$. The latter is equivalent to $n_i | a - b$. As n_i are pairwise coprime, $n = n_1 \ldots n_r | a - b$, so b, a belong to the same residue class modulo n.

□

By the Chinese Remainder Theorem solving a congruence modulo a composite number is reducible to solving the same congruence modulo its prime power factors.

1.6 Systems of Linear Congruences

Let n be a positive integer, A be a matrix of size $m \times t$ with integer entries, and a column vector of length m. One may apply Gaussian elimination to find a solution to the system

$$Ax \equiv a \,(\mathrm{mod}\, n) \tag{3}$$

or factor n if it is composite. Let A_i and $A_{i,j}$ denote the i-th row of A and the entry of the matrix in the i-row and j-th respectively. One says a matrix A is in row echelon form if there is a number $r \leq m$ and $1 \leq t_1 < t_2 < \ldots < t_r < t_{r+1} = t + 1$ such that $A_{i,j} = 0$ for $1 \leq j < t_i$ and $A_{i,t_i} = 1$, and $A_{i,j} = 0$ for $r + 1 \leq i \leq m, 1 \leq j \leq t$. The shape of the matrix in row echelon form is below

$$\begin{pmatrix} 0 \ldots 01z \ldots zzz \ldots zz \ldots z \\ 0 \ldots 000 \ldots 01z \ldots zz \ldots z \\ \ldots \\ 0 \ldots 000 \ldots 000 \ldots 01 \ldots z \\ 0 \ldots 000 \ldots 000 \ldots 00 \ldots 0 \end{pmatrix},$$

where by z undefined entries of the matrix are denoted. The elimination is based on two operations: adding to a row another row multiplied by a constant and exchanging two rows. With a combination of these operations(applied to the column a as well) one reduces the equation (3) to $A'x = a'$, where A' is in

row echelon form, or factor n. Let $M = A, a$ be a concatenation of A and the column a, so that M is a matrix of size $m \times (t+1)$.

1. Initialise $r = 0, t_r = 0$.
2. For j from $t_r + 1$ to t and for i from $r+1$ to m do:
   (a) If $b = M_{i,j} \neq 0 (\mathrm{mod}\, n)$, then compute integers z, y such that $zb + yn = d$, where $d = \gcd(b, n)$. If $d \neq 1$, then terminate, $n = d \times (n/d)$ is a factorisation of n. If $d = 1$, then $zb \equiv 1 (\mathrm{mod}\, n)$.
   (b) Exchange $M_{r+1} \leftrightarrow M_i$ and set $M_{r+1} \leftarrow zM_{r+1} (\mathrm{mod}\, n)$.
   (c) For u from $r+2$ to m do $M_u \leftarrow M_u - M_{u,j} M_{r+1}$.
   (d) Break i and j-loops.
   (e) If $M_{i,j} = 0 \,(\mathrm{mod}\, n)$, then continue. If $M_{i,j} \equiv 0 \,(\mathrm{mod}\, n)$ for $t_r + 1 \leq j \leq t$ and for $r + 1 \leq i \leq m$, then terminate.
3. If $r = m$, then terminate, else $r \leftarrow r+1$ and $t_r \leftarrow j$, repeat the step 2.

The system has a solution if and only if $M_{i,t+1} = 0$, $r+1 \leq i \leq m$. The number of solutions in residues modulo n is n^{t-r}. One generates a solution $x = (x_1, \ldots, x_t)$ to (3) with the following routine. The variables x_j, where $t_i < j < t_{i+1}$ and $1 \leq i \leq r$, may have any values modulo n. Then for i from r to 1(in this order) do:

$$x_{t_i} \equiv M_{i,t+1} - \sum_{j=t_i+1}^{t} x_j M_{i,j} \,(\mathrm{mod}\, n).$$

If a factorisation $n = n_1 n_2$, where $\gcd(n_1, n_2) = 1$, is known, one can solve $Ax_i \equiv a \,(\mathrm{mod}\, n_i)$ and reconstruct a solution $x (\mathrm{mod}\, n)$ from $x_i (\mathrm{mod}\, n_i)$, $i = 1, 2$ with the Chinese Remainder Theorem. If $n = p^l$, where p is prime and $l > 1$, then computing a solution to (3) is a bit more tricky and not considered here.

Assume we need to solve

$$\begin{pmatrix} 1 & 2 & -2 & 0 \\ -1 & 0 & 0 & 1 \\ 0 & 2 & -1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} (\mathrm{mod}\, 15).$$

One concatenates the matrix and the right hand side column. A sequence of row transformations is then applied.

$$\begin{pmatrix} 1 & 2 & -2 & 0 & 1 \\ -1 & 0 & 0 & 1 & 1 \\ 0 & 2 & -1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & -2 & 0 & 1 \\ 0 & 2 & -2 & 1 & 2 \\ 0 & 2 & -1 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & -2 & 0 & 1 \\ 0 & 1 & -1 & 8 & 1 \\ 0 & 2 & -1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & -2 & 0 & 1 \\ 0 & 1 & -1 & 8 & 1 \\ 0 & 0 & 1 & -1 & -1 \end{pmatrix}.$$

The system has 15 solutions. All of them are generated by setting to x_4 any residue modulo 15 and the values of all other variables x_1, x_2, x_3 are computed in a unique way. For instance, let $x_4 = 0$. Then $x_3 = -1 + x_4 = -1, x_2 = 1 + x_3 - 8x_4 = 0, x_1 = 1 - 2x_2 + 2x_3 = -1$. So $(-1, 0, -1, 0)$ is a solution. We have not factored the module as the inversion modulo 15 was always possible.

1.7 Euler's and Fermat's Theorems

Theorem 16. *(Fermat's "little" theorem) Let p be prime and a be an integer not multiple of p. Then $a^{p-1} \equiv 1 (mod p)$.*

Proof. Since $\gcd(a, p) = 1$ the residues $ai (\mathrm{mod}\, p), 1 \leq i \leq p-1$ are permuted numbers $1, \ldots, p-1$. Therefore

$$a^{p-1}(\prod_{i=1}^{p-1} i) = \prod_{i=1}^{p-1} ai \equiv (\prod_{i=1}^{p-1} i) (\mathrm{mod}\, p).$$

Then $\gcd(\prod_{i=1}^{p-1} i, p) = 1$ because p is prime. By Theorem 13, we can cancel the product on the both sides of the congruence. Hence $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. □

This theorem implies $a^p \equiv a (\mathrm{mod}\, p)$ for any integer a.

Corollary 3. *Let p be prime and e, f, a be integer numbers such that $e \equiv f (mod\, p-1)$. Then $a^e \equiv a^f (mod p)$.*

Proof. Since $e \equiv f (\mathrm{mod}\, p-1)$ we can write $e = f + (p-1)k$ for some integer k. Therefore by Fermat's theorem,

$$a^e = a^{f+(p-1)k} = a^f (a^{(p-1)})^k \equiv a^f 1^k \equiv a^f (\mathrm{mod}\, p).$$

□

We apply the theorem for computing the lowest decimal digit x of 3^{1234}. In other words, we need to find x such that $3^{1234} \equiv x (\mathrm{mod}\, 10)$. As $10 = 5 \cdot 2$, we will compute 3^{1234} modulo 5 and modulo 2 and then find x with the Chinese Remainder Theorem. It is easy to see that $3^{1234} \equiv 1 (\mathrm{mod}\, 2)$. Then $1234 (\mathrm{mod}\, 4) \equiv 2$. As $4 = 5 - 1$, by Corollary 3, $3^{1234} \equiv 3^2 \equiv 4 (\mathrm{mod}\, 5)$. One then finds x from $x \equiv 1 (\mathrm{mod}\, 2)$ and $x \equiv 4 (\mathrm{mod}\, 5)$, that is $x = 9$.

We now study Euler's theorem. Let n be a positive integer number. We remark that if $a \equiv b (\mathrm{mod}\, n)$, then $\gcd(a, n) = \gcd(b, n)$. The number of residues a coprime with n is called Euler totient function of n and denoted $\phi(n)$. In other words, $\phi(n)$ is the number of a in $1 \leq a < n$ such that $\gcd(a, n) = 1$. By agreement, $\phi(1) = 1$.

Lemma 3. *Let $x_1, \ldots, x_{\phi(n)}$ be all different residues(from different residue classes) modulo n coprime to n, and a is coprime to n. Then $ax_1, \ldots, ax_{\phi(n)}$ are all different residues modulo n.*

Proof. Suppose, by contrary, the residues of $ax_1, \ldots, ax_{\phi(n)}$ are not different pairwise. That is $ax_i \equiv ax_j (\mathrm{mod}\, n), i \neq j$. By Theorem 13, $x_i \equiv x_j (\mathrm{mod}\, n)$ which is a contradiction. □

Theorem 17. *(Euler's theorem) Let $n > 1$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 (mod\, n)$.*

Proof. Let $x_1, \ldots, x_{\phi(n)}$ be all different residues(from different residue classes) modulo n coprime to n. By Lemma 3, $ax_1, \ldots, ax_{\phi(n)}$ are all different residues modulo n coprime to n. Therefore,

$$a^{\phi(n)} \left(\prod_{i=1}^{\phi(n)} x_i \right) = \prod_{i=1}^{\phi(n)} ax_i \equiv \left(\prod_{i=1}^{\phi(n)} x_i \right) (\mathrm{mod}\, n).$$

As $\gcd(\prod_{i=1}^{\phi(n)} x_i, n) = 1$, by Theorem 13, we can cancel the product on the both sides of the congruence. Hence $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$. □

Corollary 4. *Let $n > 1$ be an integer and e, f, a be integer numbers such that $e \equiv f (mod\ \phi(n))$ and $\gcd(a, n) = 1$. Then $a^e \equiv a^f (mod\, n)$.*

Proof. Since $e \equiv f (\mathrm{mod}\ \phi(n))$ we can write $e = f + \phi(n)k$ for some integer k. Therefore by Fermat's theorem,

$$a^e = a^{f+\phi(n)k} = a^f (a^{\phi(n)})^k \equiv a^f 1^k \equiv a^f (\mathrm{mod}\, n).$$

□

We apply the theorem for computing the lowest decimal digit x of 3^{1234}. We realise that $1, 3, 7, 9$ are all residues modulo 10 coprime to 10, so $\phi(10) = 4$. By division with remainder, $1234 \equiv 2 (\mathrm{mod}\, 4)$. By Corollary 4, $x \equiv 3^{1234} \equiv 3^2 = 9 (\mathrm{mod}\, 10)$.

Theorem 18. *Let m, n be coprime positive integers, then $\phi(mn) = \phi(n)\phi(m)$.*

Proof. Let $R(n)$ be all residues modulo n coprime with n. We construct a one-to-one correspondence (bijection) between $R(nm)$ and $R(n) \times R(m)$. That will prove $\phi(mn) = \phi(n)\phi(m)$. Let $f : R(nm) \to R(n) \times R(m)$ be a function defined by

$$f(x) = (a, b) = (x (\mathrm{mod}\, n), x (\mathrm{mod}\, m)).$$

The function f is well defined as $\gcd(x, nm) = 1$ implies $\gcd(x (\mathrm{mod}\, m), m) = \gcd(x, m) = 1$ and, similarly, $\gcd(x (\mathrm{mod}\, n), n) = \gcd(x, n) = 1$. The Chinese Remainder Theorem says that

$$x \equiv a (\mathrm{mod}\, n),\ x \equiv b (\mathrm{mod}\, m)$$

has exactly one solution $x (\mathrm{mod}\, nm)$ for any residues $a \in R(n), b \in R(m)$. That implies f is a one-to-one correspondence. □

Theorem 19. *Let p be a prime and n, e be integers > 1. Then*

1. $\phi(p) = p - 1$,
2. $\phi(p^e) = p^e - p^{e-1}$,
3. *if $n = \prod_{i=1}^{k} p_i^{e_i}$, then $\phi(n) = \prod_{i=1}^{k} p_i^{e_i} - p_i^{e_i - 1} = n \prod_{i=1}^{k} (1 - 1/p_i)$, the product over all prime factors p of n.*

Proof. 1. The numbers $1, \ldots, p-1$ are all residues modulo p coprime to p. So $\phi(p) = p - 1$.

2. The residues modulo p^e are $0, 1, \ldots, p^e - 1$. Only $0, p, 2p, \ldots, (p^{e-1} - 1)p$ among them have a common factor with p^e. So $\phi(p^e) = p^e - p^{e-1}$.

3. By Theorem 18,

$$\begin{aligned} \phi(n) &= \phi\left(\prod_{i=1}^{k} p_i^{e_i}\right) = \prod_{i=1}^{k} \phi(p_i^{e_i}) = \prod_{i=1}^{k} (p_i^{e_i} - p_i^{e_i - 1}) \\ &= \prod_{i=1}^{k} p_i^{e_i} \prod_{i=1}^{k} (1 - 1/p_i) = n \prod_{i=1}^{k} (1 - 1/p_i). \end{aligned}$$

□

Let $\gcd(a, n) = 1$. The order of a modulo $n > 1$ is the smallest positive integer e such that $a^e \equiv 1 (\mathrm{mod}\, n)$.

Theorem 20. *Let $\gcd(a, n) = 1$ and e be the order of a modulo n. Then $a^x \equiv 1 (mod\, n)$ if and only if $e|x$.*

Proof. If $e|x$, then $x = ek$ for some k and so $a^x \equiv (a^e)^k \equiv 1^k \equiv 1 (\mathrm{mod}\, n)$. Assume $a^x \equiv 1 (\mathrm{mod}\, n)$. By division with remainder, $x = eq + r$, where $0 \leq r < e$. Then $1 \equiv a^x \equiv a^{eq+r} \equiv (a^e)^q a^r \equiv a^r (\mathrm{mod}\, n)$. If $r > 0$ this is a contradiction with the fact that e is the smallest positive number such that $a^e \equiv 1 (\mathrm{mod}\, n)$. So $r = 0$ and $e|x$.

□

1.8 Primitive roots

Let $\gcd(a, n) = 1$. An integer a whose order modulo n is $\phi(n)$ is called a primitive root modulo n. If a is a primitive root, then a^k is a primitive root too whenever $\gcd(k, \phi(n)) = 1$).

Theorem 21. *There exist primitive roots modulo n if and only if n is one of $2, 4, p^e, 2p^e$, where p is an odd prime number.*

We take this statement without proof and consider examples. As $\phi(2) = 1$, the residue 1 is a primitive root modulo $n = 2$. For $n = 3$ we have $\phi(3) = 2$ and 2 is a primitive root modulo 3. Let $n = 4$, then $\phi(4) = 2$ and 3 is a primitive root. Let $n = 5$, then $\phi(5) = 4$ and 2 is a primitive root. Let $n = 6$, then $\phi(6) = 2$ and 5 is a primitive root. There are no primitive roots for $n = 8$ as $\phi(8) = 4$ and for every odd residue a (that is coprime to 8) we have $a^2 \equiv 1(\mathrm{mod}\, 8)$. One can use the following test to find a primitive root modulo n. Let $p_1, \ldots, p_k$ be all different prime divisors of $\phi(n)$.

Theorem 22. *Let* $\gcd(a, n) = 1$. *An integer* a *is a primitive root modulo* n *if and only if*

$$a^{\phi(n)/p} \neq 1(mod\, n)$$

for all different primes $p|\phi(n)$.

Proof. Let e be the order of a modulo n. Then $e|\phi(n)$ by Theorem 20. We realise $e < \phi(n)$ if and only if $\phi(n) = ek = eps$, where $k = ps$ and p is a prime number. So a is not a primitive root if and only if $e < \phi(n)$ and that holds if and only if $a^{\phi(n)/p} \equiv 1(\mathrm{mod}\, n)$ for some prime number $p|\phi(n)$. Equivalently, a is a primitive root if and only if $a^{\phi(n)/p} \neq 1(\mathrm{mod}\, n)$ for any prime divisor p of $\phi(n)$. □

Theorem 23. *Let* $\gcd(a, n) = 1$ *and* a *has order* e *modulo* n. *Then* $a^i \equiv a^j(mod\, n)$ *if and only if* $i \equiv j(mod\, e)$.

Proof. We have $i \equiv j(\mathrm{mod}\, e)$ if and only if $i = j + ek$ for some integer k. The latter implies

$$a^i \equiv a^{j+ek} \equiv a^j(a^e)^k \equiv a^j 1^k \equiv a^j(\mathrm{mod}\, n).$$

Conversely, let $a^i \equiv a^j(\mathrm{mod}\, n)$. We can assume $i \geq j$, then $a^{i-j} \equiv 1(\mathrm{mod}\, n)$. By Theorem 20, $e|(i - j)$. So $i \equiv j(\mathrm{mod}\, e)$. □

Corollary 5. *Let* $\gcd(a, n) = 1$ *and* a *has order* e *modulo* n. *Then the powers* $1, a, a^2, \ldots, a^{e-1}$ *are all different modulo* n.

Proof. Really, if $a^i \equiv a^j(\mathrm{mod}\, n)$, then by Theorem 23, we have $i \equiv j(\mathrm{mod}\, e)$. The latter is impossible as $0 \leq i < j \leq e - 1$. □

Theorem 24. *Let* g *be a primitive root modulo* n *and* a *coprime to* n. *Then there is exactly one exponent* k *in* $0 \leq k < \phi(n)$ *such that* $g^k \equiv a(mod\, n)$.

The statement holds by Corollary 5. The exponent k (a residue modulo $\phi(n)$) is called a discrete logarithm of a modulo n to the base g and denoted $k = \log_g(a)$. In classical Number Theory k is called index of a modulo n to the base g. The discrete logarithm keeps the main properties of ordinary logarithms. In particular, $c = a \cdot b(\mathrm{mod}\, n)$ if and only if $\log_g(c) = \log_g(a) + \log_g(b)\,(\mathrm{mod}\, \phi(n))$, where a, b are any integers coprime to n.

Given an integer number a and positive integer numbers x, n, the algorithm below computes $b \equiv a^x(\mathrm{mod}\, n)$.

1. Compute binary expansion $x = x_t 2^t + x_{t-1}2^{t-1} + \ldots + x_0, \quad x_t = 1.$

2. Set $b = a$. For i from $t-1$ to 0(in this order) do $b \leftarrow b^2 * a^{x_i}$.

The algorithm takes t squarings and at most t multiplications by a.

1.9 Quadratic Congruences

In this section we study how to solve

$$x^2 \equiv a(\mathrm{mod}\, n), \tag{4}$$

that is given a, n we are to find x. That is useful in primality testing and analysis of some public key cryptosystems studied later. If a is coprime with n and the congruence (4) has a solution, then a is called a quadratic residue modulo n and a quadratic non-residue otherwise. For instance, $1, 3, 4, 5, 9$ are all quadratic residues modulo 11 and $2, 6, 7, 8, 10$ are all quadratic non-residues modulo 11.

If the decomposition of $n = \prod_{i=1}^{t} p_i^{e_i}$ is known one may solve $x^2 \equiv a(\mathrm{mod}\, p_i^{e_i})$ and then reconstruct a solution to (4) with the Chinese Remainder Theorem. We study $x^2 \equiv a(\mathrm{mod}\, p)$, where p is a prime number. The congruence $x^2 \equiv a(\mathrm{mod}\, 2)$ has always one solution $x \equiv a(\mathrm{mod}\, 2)$.

Theorem 25. *Let p be prime. Then $x^2 \equiv 1(mod\, p)$ if and only if $x \equiv \pm 1(mod\, p)$.*

Proof. We may write $x^2 - 1 = (x-1)(x+1) \equiv 0(\mathrm{mod}\, p)$. In other words, $p|(x-1)(x+1)$. By Lemma 2, $p|(x-1)$ or $p|(x+1)$. So $x \equiv 1(\mathrm{mod}\, p)$ or $x \equiv -1(\mathrm{mod}\, p)$. □

Corollary 6. *Let g be a primitive root modulo an odd prime number p, then $g^{(p-1)/2} \equiv -1(mod\, p)$.*

Proof. Let $x \equiv g^{(p-1)/2}(\mathrm{mod}\, p)$, then $x^2 \equiv 1(\mathrm{mod}\, p)$. By Theorem 25, $x \equiv \pm 1(\mathrm{mod}\, p)$. If $x \equiv 1(\mathrm{mod}\, p)$, then $g^{(p-1)/2} \equiv 1(\mathrm{mod}\, p)$ and g cannot be a primitive root as the order of g is $< p-1$ in this case. So $x \equiv -1(\mathrm{mod}\, p)$. □

Theorem 26. *Let p be an odd prime and $a \neq 0(mod\, p)$. Then $x^2 \equiv a(mod\, p)$ has either no solutions or exactly two incongruent solutions.*

Proof. If x is a solution then $-x$ is a solution too. Those solutions are incongruent, otherwise $x \equiv -x(\mathrm{mod}\, p)$ which is equivalent to $p|2x$ and so $p|x$. Then $a \equiv x^2 \equiv 0(\mathrm{mod}\, p)$ which is a contradiction. Assume a third solution b, besides $\pm x$. Then from $b^2 \equiv a(\mathrm{mod}\, p)$ and $x^2 \equiv a(\mathrm{mod}\, p)$ one gets $b^2 \equiv x^2(\mathrm{mod}\, p)$ which is equivalent to $p|b^2 - x^2 = (b-x)(b+x)$. Hence $b \equiv x$ or $b \equiv -x$ modulo p and there are only two solutions. □

Theorem 27. *Let p be an odd prime number. There are exactly $(p-1)/2$ quadratic residues among $1, 2, \ldots, p-1$ and the same number of quadratic non-residues.*

Proof. Every x from $1, 2, \ldots, p-1$ satisfies $x^2 \equiv a (\mathrm{mod}\, p)$ for some a from the same set. For each a there are 2 solutions $\pm x (\mathrm{mod}\, p)$. Therefore the number of quadratic residues is $(p-1)/2$. Therest $(p-1)/2$ are quadratic non-residues. □

Let g be a primitive root modulo an odd p, then the quadratic residues are exactly even powers of g modulo p.

1.10 Legendre Symbol

Let p be an odd prime number and a be an integer. We define the Legendre symbol (a/p). We set $(a/p) = 1$ if a is a quadratic residue (mod p) and $(a/p) = -1$ if a is a quadratic non-residue, and $(a/p) = 0$ if $a \equiv 0 (\mathrm{mod}\, p)$. The following theorem was proved by Euler.

Theorem 28. $(a/p) \equiv a^{(p-1)/2}$.

Proof. By Theorem 21, there is a primitive root g modulo p. Then the even powers $g^0, g^2, g^4, \ldots, g^{p-1}$ of g are all quadratic residues modulo p and there are $(p-1)/2$ of them. The odd powers $g^1, g^3, \ldots, g^{p-2}$ are all quadratic non-residues. If a is a quadratic residue, then $a = g^{2k}$ and $a^{(p-1)/2} \equiv g^{(p-1)k} \equiv 1 (\mathrm{mod}\, p)$. If a is a quadratic non-residue, then $a = g^{2k+1}$ and $a^{(p-1)/2} \equiv g^{(p-1)k+(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$, as $g^{(p-1)/2} \equiv -1 (\mathrm{mod}\, p)$ by Corollary 6. Anyway, $(a/p) \equiv a^{(p-1)/2}$. □

We list useful properties of the Legendre symbol.

Theorem 29. *Let p be an odd prime number and a, b be integers.*

1. *The number of solutions to the congruence $x^2 \equiv a (mod\, p)$ is $1 + (a/p)$,*
2. *$(a/p) \equiv a^{(p-1)/2}$,*
3. *$(ab/p) = (a/p)(b/p)$,*
4. *if $a \equiv b (mod\, p)$, then $(a/p) = (b/p)$,*
5. *$(1/p) = 1$ and $(-1/p) = (-1)^{(p-1)/2}$. Equivalently, -1 is a quadratic residue modulo p if and only if $p \equiv 1 (mod\, 4)$.*
6. *if p does not divide a, then $(a^2/p) = 1$ and $(a^2 b/p) = (b/p)$.*

1.11 The Law of Quadratic Reciprocity

The following theorem states the law of quadratic reciprocity proved by Gauss.

Theorem 30. *Let p, q be distinct odd prime numbers, then*

1. $(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$,
2. $(2/p) = (-1)^{\frac{p^2-1}{8}}$.

The second statement of the theorem implies that the congruence $x^2 \equiv 2 \pmod{p}$ is solvable if $p \equiv 1$ or 7 and not solvable if $p \equiv 3$ or 5 modulo 8. Really, let $p = 8k+r$, where r is one of $1, 3, 5, 7$. Then $p^2-1 = (8k+r)^2-1 = r^2-1+16s$ for some s. So $\frac{p^2-1}{8}$ is even for $r = 1, 7$ and odd for $r = 3, 5$.

Assume we are to decide if a congruence $x^2 \equiv a \pmod{p}$ is solvable. We need to compute (a/p). The latter may be done by computing $(a/p) \equiv a^{(p-1)/2} \pmod{p}$ via exponentiation or with Quadratic Reciprocity Law. For instance, let $x^2 \equiv -22 \pmod{59}$. As $-22 = -1 \cdot 2 \cdot 11$,

$$(-22/59) = (-1/59)\,(2/59)\,(11/59) = (-1)(-1)(-1) = -1,$$

as by Theorem 29, $(-1/59) = (-1)^{(59-1)/2} = -1$. By Theorem 32, we have $(2/59) = -1$ as $59 \equiv 3 \pmod{8}$. By the same theorem,

$$(11/59) = (4/11)(-1)^{\frac{59-1}{2}\frac{11-1}{2}} = -(2^2/11) = -(2/11)^2 = -1.$$

We conclude the congruence $x^2 \equiv -22 \pmod{59}$ is unsolvable. The application of the Quadratic Reciprocity Law often requires factoring which may be difficult for large numbers.

1.12 Jacobi Symbol

Let n be an odd positive integer and $n = \prod_{i=1}^{k} p_i^{e_i}$, and a be an integer. The Jacobi symbol (a/n) is defined by

$$(a/n) = \prod_{i=1}^{k} (a/p_i)^{e_i},$$

where (a/p_i) are Legendre symbols. By agreement, $(a/1) = 1$. If $\gcd(a, n) > 1$, then $(a/p_i) = 0$ for some p_i so, by the definition above, $(a/n) = 0$. By the definition and the properties of the Legendre symbol we get the following properties of the Jacobi symbol.

Theorem 31. *Let n, m be an odd positive integers and a, b be integers.*

1. *If $a \equiv b (mod n)$, then $(a/n) = (b/n)$.*
2. *$(ab/n) = (a/n)(b/n)$,*
3. *$(a/nm) = (a/n)(a/m)$,*
4. *if $\gcd(a, n) = 1$, then $(a^2/n) = (a/n^2) = 1$, $(a^2b/n) = (b/n)$, and $(b/m^2n) = (b/n)$.*

The following theorem states the Law of Quadratic Reciprocity for Jacobi symbols.

Theorem 32. *Let n, m be odd coprime integers, then*

1. $(m/n)(n/m) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$,

2. $(2/n) = (-1)^{\frac{n^2-1}{8}}$.

3. $(-1/n) = (-1)^{\frac{n-1}{2}}$.

Proof. We will prove the last statement, the first two statement are proved similarly. Let $n = \prod_{i=1}^{k} p_i^{e_i}$. By the definition of Jacobi symbol and Theorem 31,

$$(-1/n) = \prod_{i=1}^{k} (-1/p_i)^{e_i} = (-1)^s,$$

where $s = \sum_{i=1}^{k} e_i(p_i - 1)/2$ as $(-1/p_i) = (-1)^{(p_i-1)/2}$. As $p_i - 1$ is even, we get

$$n = \prod_{i=1}^{k} (1 + (p_i - 1))^{e_i} \equiv 1 + \sum_{i=1}^{k} e_i(p_i - 1) (\mathrm{mod}\, 4).$$

Hence, $(n-1)/2 \equiv s (\mathrm{mod}\, 2)$ and $(-1/n) = (-1)^{(n-1)/2}$.

□

With Theorem 32 one computes Jacobi and Legendre symbols without factoring. One can compute (a/n) recursively by the following steps.

1. Set $a \leftarrow a (\mathrm{mod}\, n)$, so $0 \leq a < n$. If $a = 0$, then $(a/n) = 0$. If $a = 1$, then $(a/n) = 1$. Terminate. Else $a = 2^s b$, where b is an odd number and $s \geq 0$.

2. Represent

$$(a/n) = (2^s b/n) = (2/n)^s (b/n) = \\ (-1)^{s(n^2-1)/8 + (b-1)(n-1)/4} (n/b).$$

3. If $b = 1$, then terminate, else to compute (n/b), set $a \leftarrow n, n \leftarrow b$ and repeat the first step.

Let's compute the Legendre symbol $(-22/59)$ with the algorithm above.

$$(-22/59) = (37/59) = (59/37) = (22/37) = (2/37)(11/37) = \\ = -(11/37) = -(37/11) = -(4/11) = -1.$$

1.13 Solving Quadratic Congruences Modulo Primes

The congruence $x^2 \equiv a (\mathrm{mod}\, p)$, where a is coprime to p, has a solution if and only if the Legendre symbol $(a/p) = 1$. We now show how to explicitly compute a solution if it exists.

Theorem 33. *Let $p \equiv 3 (mod\, 4)$ and a be a quadratic residue modulo p. Then the solutions to $x^2 \equiv a (mod\, p)$ are $x \equiv \pm a^{(p+1)/4}$.*

Proof.

$$x^2 \equiv a^{(p+1)/2} \equiv aa^{(p-1)/2} \equiv a(a/p) \equiv a(\mathrm{mod}\, p)$$

as by Euler's theorem $a^{(p-1)/2} \equiv (a/p)(\mathrm{mod}\, p)$ and $(a/p) = 1$. □

Assume a is a quadratic residue modulo p. The following algorithm computes the solutions to $x^2 \equiv a(\mathrm{mod}\, p)$.

1. Let $p - 1 = 2^k h$, where $h = 2h_1 + 1$ is odd and $k \geq 1$.
2. Generate a quadratic non-residue g modulo p and set $d \equiv g^h(\mathrm{mod}\, p)$. Remark that the order of d is exactly 2^k, that is $d^{2^k} \equiv 1(\mathrm{mod}\, p)$ and $d^{2^{k-1}} \neq 1(\mathrm{mod}\, p)$.
3. Find an integer r (see below) such that $a^h \equiv d^{2r}(\mathrm{mod}\, p)$ and set $x \equiv a^{-h_1} d^r(\mathrm{mod}\, p)$. Terminate.

As

$$x^2 \equiv (a^{-h_1} d^r)^2 \equiv a^{-2h_1} d^{2r} \equiv a^{-2h_1+h} \equiv a(\mathrm{mod}\, p),$$

the algorithm solves the problem. For constructing a non-residue g a random residue may be tested with Euler's theorem.

As a is a quadratic residue, then the order of $a_1 = a^{th}$ is a factor of 2^{k-1}, that is $a_1^{2^{k-1}} \equiv 1(\mathrm{mod}\, p)$. All such residues are powers of $d_1 = d^2$, so one has $a_1 = d_1^r$ for some integer $0 \leq r < 2^{k-1}$. In other words, r is the discrete logarithm of a_1 in the group of residues modulo p generated by $d_1 = d^2$. The logarithm r may be efficiently computed with at most $k - 1$ trials by the following method.

We will find the first binary digit $r_0 \in \{0, 1\}$ of $r = r_0 + r'2$ by testing: $r_0 = 0$ if and only if

$$(a_1)^{2^{k-2}} \equiv 1(\mathrm{mod}\, p).$$

One puts $a_2 = a_1 d_1^{-r_0}$ and $d_2 = d_1^2$ and has to find $0 \leq r' < 2^{k-2}$ such that $a_2 = d_2^{r'}$ in a subgroup of residues modulo p of size 2^{k-2}. One recursively applies the same method thus finding all binary digits of r.

For instance, let $p = 17$ and $a = 2$. By Theorem 32, $(2/17) = (-1)^{(17^2-1)/8} = 1$, so the congruence $x^2 \equiv 2(\mathrm{mod}\, 17)$ has a solution.

We have $17 - 1 = 2^4$, so $h = 1$ and $0 \cdot 2 + 1 \cdot 1 = 1$ $(s = 0, t = 1)$. By computing a Jacobi symbol, one finds $g = 3$ is a quadratic non-residue, so $d \equiv 3$ and one has to find $r(\mathrm{mod}\, 2^3) \equiv r_0 + r_1 2 + r_2 2^2$ such that

$$a_1 \equiv 2 \equiv 3^{2r} \equiv 9^{r_0 + r_1 2 + r_2 2^2}(\mathrm{mod}\, 17).$$

As $a_1^{2^2} \equiv 2^{2^2} \equiv -1(\mathrm{mod}\, 17)$, one concludes $r_0 = 1$. Then

$$a_2 = 2 \cdot 9^{-1} \equiv 4 \equiv 9^{r_1 2 + r_2 2^2} = 13^{r_1 + r_2 2},$$

where $9^2 \equiv 13(\mathrm{mod}\, 17)$. As $a_2^{2^1} \equiv -1(\mathrm{mod}\, 17)$, one concludes $r_1 = 1$. Then

$$a_3 = 4 \cdot 13^{-1} \equiv 16 \equiv 13^{r_2 2} = 16^{r_2},$$

where $13^2 \equiv 16(\mathrm{mod}\, 17)$. As $a_3^{2^0} \equiv -1(\mathrm{mod}\, 17)$, one concludes $r_2 = 1$. Hence, $r = 7$ and we set $x \equiv 2^s 3^r \equiv 3^7 \equiv 11(\mathrm{mod}\, 17)$. Therefore, ± 11 are the solutions to the congruence $x^2 \equiv 2(\mathrm{mod}\, 17)$.

1.14 Polynomial Equations Modulo Primes

A polynomial is the function $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$. If $a_d \neq 0$ then d is called the degree of f.

Theorem 34. *Let p be prime and $f(x)$ be a polynomial with integer coefficients of degree $d \geq 1$ modulo p (that is d is the largest index such that $a_d \neq 0 (mod\, p)$). Then the congruence $f(x) \equiv 0 (mod\, p)$ has at most d solutions.*

Proof. We will use induction. Let $d = 1$, then the congruence $a_1 x + a_0 \equiv 0 (\mathrm{mod}\, p)$ has exactly one solution by Corollary 2. The theorem statement is correct in this case. Assume the theorem is true for all polynomial congruences of degree $< d$. Suppose that the congruence $f(x) \equiv 0 (\mathrm{mod}\, p)$ of degree d has at least $d+1$ incongruent solutions: $r_1, \ldots, r_d, r_{d+1}$. Let's define a new polynomial

$$g(x) = f(x) - a_d(x - r_1)\ldots(x - r_d).$$

The degree g is $< d$ as the term $a_d x^d$ cancels when subtracting. By induction, the congruence $g(x) \equiv 0 (\mathrm{mod}\, p)$ has $< d$ solutions. However, by construction $r_1, \ldots, r_d$ are its solutions. That is only possible when $g = 0$ and therefore

$$f(x) = a_d(x - r_1)\ldots(x - r_d).$$

Then

$$0 \equiv f(r_{d+1}) = a_d(r_{d+1} - r_1)\ldots(r_{d+1} - r_d) (\mathrm{mod}\, p).$$

So p divides at least one of $a_d, (r_{d+1} - r_1), \ldots, (r_{d+1} - r_d)$ which is impossible. □

We now present an algorithm to compute the solutions to the congruence $f(x) \equiv 0 (\mathrm{mod}\, p)$ of degree d. The method is efficient for relatively small d. Input to the algorithm is a polynomial f with integer coefficients and a prime number p. Output is a residue $r (\mathrm{mod}\, p)$ such that $f(r) \equiv 0 (\mathrm{mod}\, p)$ or the message that the congruence has no solutions in residues modulo p. The coefficients of the intermediate polynomials are reduced modulo p when computing with this algorithm.

1. Compute $h(x) \equiv x^p - x \,(\mathrm{mod}\, f(x))$ by first computing $x^p (\mathrm{mod}\, f(x))$ with the binary method of exponentiation. Set

   $$g(x) \leftarrow \gcd(x^p - x, f(x)) = \gcd(h(x), f(x)).$$

   We assume that the leading coefficient of $g(x)$ is 1.

2. If $g(x) = 1$, then the congruence has no solutions, terminate. If $\deg g(x) = 1$, then $g(x) = x - r$ and r is a solution, terminate.

3. If $\deg g(x) \geq 2$, then take a random $b (\mathrm{mod}\, p)$. With the binary method of exponentiation compute

   $$v(x) = \gcd(g(x), (x + b)^{(p-1)/2} - 1).$$

   If $v(x) = 1$ or $g(x)$, then repeat the step. If $v(x) = x - r$, then r is a solution, terminate.

4. If $2 \leq \deg v(x) < \deg g(x)$, then set $g(x) \leftarrow v(x)$ or $g(x)/v(x)$ of the smallest degree. Go to the step 2.

The algorithm running time is determined by the number of random residues b chosen before a solution is found. We estimate the probability P that the polynomial $v(x)$ is a proper divisor of $g(x)$, that is $\deg v(x) < \deg g(x)$. In this case a solution is found or the degree of $g(x)$ got reduced by half. The following lemma is a corollary of Fermat's "little" theorem.

Lemma 4. *$x^p - x = \prod_r (x - r)$, where the product is over all residues r modulo p.*

The lemma implies that $g(x) = (x - r_1) \dots (x - r_s)$ for some different residues $r_1, \dots, r_s$ modulo p, where $s \geq 2$. The probability P is at least the probability that exactly one of r_1, r_2 is a solution to the congruence $v(x) \equiv 0 (\mathrm{mod}\, p)$. In that case $v(x)$ is a proper divisor of $g(x)$. We will estimate P.

Let D be all residues b such that

$$b \neq -r_1, r_2 \,(\mathrm{mod}\, p),$$
$$(r_1 + b)^{(p-1)/2} - (r_2 + b)^{(p-1)/2} \neq 0 (\mathrm{mod}\, p).$$

If $b \in D$, then exactly one of r_1, r_2 is a root of the polynomial $(x + b)^{(p-1)/2} - 1$ and therefore of the polynomial $v(x) = \gcd(g(x), (x + b)^{(p-1)/2} - 1)$. Really, as $(r_1 + b)^{(p-1)/2} \equiv \pm 1$, then $(r_2 + b)^{(p-1)/2} \equiv \mp 1$.

Lemma 5. $|D| \geq (p - 1)/2$.

Proof. Let D_1 be the set of solutions of the congruence

$$F(x) = (r_1 + x)^{(p-1)/2} - (r_2 + x)^{(p-1)/2} \equiv 0 (\mathrm{mod}\, p)$$

The polynomial $F(x)$ is of degree $\leq (p-3)/2$. By Theorem 34, $|D_1| \leq (p-3)/2$. Now $D \cup D_1 \cup \{r_1, r_2\}$ are all different residues modulo p. So

$$p = |D| + |D_1| + 2.$$

So $|D| = p - |D_1| - 2 \geq p - (p - 3)/2 - 2 = (p - 1)/2$. □

The lemma implies that $P \geq (p - 1)/2p$. Therefore for large p with probability close to $1/2$ one finds a solution or reduces the degree of $g(x)$ by half. The degree of the initial $g(x)$ is at most d. So the average number of steps before one gets a linear polynomial $g(x) = x - r$ and therefore a solution r is $2 \log_2 d$. Remark that the multiplication and the division of the polynomials of degree $\leq d$ takes $O(d^2)$ arithmetic operations modulo p and the exponentiation takes $O(d^3)$. Overall complexity is then $O(d^3 \log d)$.

We apply the algorithm to $p = 43$ and $f(x) = x^4 + 38x^3 + 9x^2 + 36x + 2$. One computes

$$g(x) = \gcd(x^p - x, f(x)) = x^2 + 40x + 2.$$

Therefore all residues which satisfy $f(x) \equiv 0 (\mathrm{mod}\, 43)$ will satisfy $g(x) \equiv 0 (\mathrm{mod}\, 43)$. One randomly chooses $b = 9$ and finds that

$$x^2 + 40x + 2 = \gcd(x^2 + 40x + 2, (x + 9)^{(p-1)/2} - 1).$$

That does not give any solution. One randomly chooses $b = 33$ and gets

$$x + 41 = \gcd(x^2 + 40x + 2, (x + 33)^{(p-1)/2} - 1).$$

Therefore, $x = -41 \equiv 2 (\mathrm{mod}\, 43)$ is a solution to $f(x) \equiv 0 (\mathrm{mod}\, 43)$.

1.15 Primality Testing

Let n be an odd positive integer number and a be an integer. Obviously, if $a^{n-1} \neq 1 (\mathrm{mod}\, n)$, then n is not prime by Fermat's theorem. However, the congruence $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ does not guarantee that n is a prime number. The following theorem was proved by Pocklington.

Theorem 35. *Let $n > 1$ be an odd integer number. Assume there exist integer a and prime p such that*

1. $a^{n-1} \equiv 1 (mod\, n)$,
2. $p | n - 1$ *and* $p > \sqrt{n} - 1$,
3. $\gcd(a^{(n-1)/p} - 1, n) = 1$.

Then n is prime.

Proof. Suppose, on the contrary, that n is composite. So there is a prime $q | n$ and $q \leq \sqrt{n}$. Then $p > \sqrt{n} - 1 \geq q - 1$ and $\gcd(p, q - 1) = 1$ since p is prime. There exist integers u, s such that $up = 1 + s(q - 1)$. Therefore, $a^{up} \equiv a^{1+s(q-1)} \equiv a (\mathrm{mod}\, q)$ by Fermat's theorem. We have $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$, so $1 \equiv a^{(n-1)u} (\mathrm{mod}\, q)$ as $q | n$. This implies

$$1 \equiv a^{(n-1)u} \equiv a^{up\frac{n-1}{p}} \equiv a^{\frac{n-1}{p}} (\mathrm{mod}\, q).$$

Therefore $q | \gcd(a^{(n-1)/p} - 1, n) = 1$. That is a contradiction.

□

Remark that in most cases if n does not pass the test, then n is composite. The exception is when n divides $a^{(n-1)/p} - 1$ and the gcd in the last condition is n, then n may be prime.

One may use Theorem 35 to construct large prime numbers. Really, one sets $n = 2pt + 1$, where a prime p satisfies $p > \sqrt{n} - 1$, and t is a positive integer. One then applies the test. The prime p may be constructed with the same test for smaller parameters. For instance, let $p = 73$ and $n = 2 \cdot 73 \cdot 21 + 1 = 3067$. One randomly chooses $a = 87$. Then $87^{3066} \equiv 1 (\mathrm{mod}\, 3067)$ and $\gcd(87^{42} - 1, 3067) = 1$. Therefore, 3067 is prime.

The numbers which pass Pocklington test or similar are called provable primes, that means we are sure they are prime. An odd number n which passes the following Solovay-Strassen test (several independent tests) is called a probable prime. That is n may be composite and passes the test with some small probability.

1. Choose a random integer a in $1 < a < n$. If $\gcd(a, n) \neq 1$, then return "composite". Terminate. Else compute the Jacobi symbol (a/n).
2. If $a^{(n-1)/2} \equiv (a/n) (\mathrm{mod}\, n)$, then return "probable prime". Else return "composite". Terminate.

Theorem 36. *Let n be an odd composite number and a is a random integer in $1 < a < n$ and $\gcd(a, n) = 1$. The probability that*

$$a^{(n-1)/2} \equiv (a/n) (mod\, n) \tag{5}$$

is $< 1/2$.

Proof. Let G be the set of all residues a modulo n in $1 \leq a < n$ such that $\gcd(a, n) = 1$. Obviously, G is a group of residues modulo n. Its order is $\phi(n) < n - 1$ as n is composite. Let S be a set of $a \in G$ such that (5) holds. It is easy to see that $S \subseteq G$ is a subgroup of G. So $|S|$ divides $|G| = \phi(n)$. It is enough to prove that S is a proper subgroup of G as then

$$|S| \leq |G|/2 < (n - 1)/2.$$

Therefore the sought probability is bounded by

$$\frac{|S| - 1}{n - 2} < \frac{n - 3}{2(n - 2)} < 1/2.$$

S is a proper subgroup of G if and only if $a \in G \setminus S$ for some a. We will construct such a.

Let p be the smallest prime factor of n. We consider two cases. First, $n = pn_1$, where $n_1 > 2$ and $\gcd(p, n_1) = 1$. There exists b such that $(b/p) = -1$, for instance, b is a primitive root modulo p. By the Chinese Remainder Theorem, there exists a solution to

$$a \equiv b \,(\mathrm{mod}\, p), \quad a \equiv 1 \,(\mathrm{mod}\, n_1)$$

and $\gcd(a, n) = 1$. So $a \in G$. Then

$$(a/n) = (a/p)(a/n_1) = (b/p)(1/n_1) = -1.$$

We realise $a^{(n-1)/2} \equiv 1 (\mathrm{mod}\, n_1)$. As $n_1 | n$ the congruence $a^{(n-1)/2} \equiv (a/n) (\mathrm{mod}\, n)$ would imply $1 \equiv -1 (\mathrm{mod}\, n_1)$, which is a contradiction. Therefore, $a \in G \setminus S$.

Second, $n = p^k n_1$, where $k \geq 2$ and $\gcd(p, n_1) = 1$. Let $a = 1 + p$, then $\gcd(a, n) = 1$ as p is the smallest prime factor of n. Assume $a^{(n-1)/2} \equiv$

$(a/n)(\mathrm{mod}\, n)$. Then we square the both sides of the congruence and take that modulo $p^2|n$. One gets $(1+p)^{(n-1)} \equiv 1\,(\mathrm{mod}\, p^2)$. Therefore,

$$1 \equiv (1+p)^{(n-1)} \equiv 1 + (n-1)p\ (\mathrm{mod}\, p^2).$$

So $n-1 \equiv 0\,(\mathrm{mod}\, p)$ or $p|n-1$. That contradicts with $p|n$. Therefore, $a \in G \setminus S$. □

Let k be a positive integer. If n passes k independent (a are chosen independently) tests, the probability n is composite $< 1/2^k$. There are even more powerful tests as a Miller-Rabin test etc, where the probability of an error $< 1/4^k$ after k iterations.