Ceng 471 Cryptography

Mathematical Background
Asymmetrical Cryptography

Basic Number Theory

Asst. Prof. Dr. Serap Şahin

Izmir Institute of Technology

Basic Number Theory

- Divisibility
- Prime Numbers
- Greatest Common Divisor
- Euclid’s Algorithm and Continued Fraction
- Solving ax+by=d
- Congruences
- Chinese Remainder Theorem
- Fast Exponentiation
- Primality Testing

Divisibility

- Definition
  - Let **a,bЄZ** with **a≠0**. We say that "**a divides b**", if there is an integer **k** such that **b=a.k**.
  - This is denoted by **a|b** , another express this is that **b is multiple of a**.

$2|18$, $-3|15$, $7\nmid 18$

Divisibility

- Propositions

Let $a,b,c \in Z$

1. For every $a \neq 0$, $a \mid 0$ and $a \mid a$. Also $1 \mid b$ for every b.
2. If $a \mid b$ and $b \mid c$ then $a \mid c$.
3. If $a \mid b$ and $a \mid c$ then $a \mid (s.b+t.c)$ for all $s,t \in Z$.

Prime Numbers

- A number $p>1$ that is divisible only by 1 and itself is called “prime number”.
- An integer $n>1$ that is not prime is called “composite”, which means that n expressible as product $a.b$ of integers with $1<a,b<n$.
- A fact that known already from Euclid, is that there are infinitely many prime numbers (proved by Euclid, 1849).

Prime Numbers

- Prime Number Theorem
  - Let ∏(x) be the number of primes less than x. Then

$$\prod(x) \approx \frac{x}{\ln x} \text{ in the sense that ratio } \frac{\prod(x)}{(x/\ln x)} \to 1 \quad as \quad x \to \infty$$

In various application we will need large primes, around 100 digits. We can estimate the number of 100 digit primes;

$$\prod(10^{100}) - \prod(10^{99}) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9 \times 10^{97}$$

There are certainly enough primes.

Prime Numbers

- Theorem
  - **Every positive integer is a product of primes.** This factorization into primes is unique, up to reordering the factors.
- Lemma
  - If p is a prime and p divides a product of integers **a.b**, then either **p|a** or **p|b**. More generally, if a prime p divides a product a.b. .. z, then p must divide one of the factors a.b. .. z.

For example; when p=2, this says that if a product of two integers is even then one of the two integers must be even.

Prime Numbers

- The proof of the theorem

  $n = p_1^{a_1}.p_2^{a_2}\ldots p_s^{a_s} = q_1^{b_1}.q_2^{b_2}\ldots q_t^{b_t}$ where $p_1, p_2,.., p_s \, and \quad q_1, q_2,.., q_t$ are primes, and the exponents *a*$_i$ and *b*$_j$ are non-zero. If a prime occurs in both factorizations, divide both sides by it to obtain a shorter relation. Continuing in this way, we may assume that none of the primes $p_1, p_2,.., p_s \, occur \quad among \quad q_j's.$

Take a prime that occurs on the left side p$_1$, since p$_1$|n, which equals $n = q_1^{b_1}.q_2^{b_2}\ldots q_t^{b_t}$ the lemma says that p$_1$ must divide one of the factors *q*$_j$. Since *q*$_j$ is prime, *p*$_i$ =*q*$_j$. This contradicts the assumption that *p*$_1$ does not occur among the *q*$_j$'s. Therefore an integer cannot have two distinct factorization.

Greatest Common Divisor

- The “greatest common divisor” (GCD or gcd), of a and b is the largest positive integer dividing both a and b and is denoted by either gcd(a,b) or by (a,b).

  Examples: gcd(6,4)=2, gcd(5,7)=1, gcd(24,60)=12.
- If gcd(a,b)=1 then a and b are relatively prime.
- There are two standard ways to find the gcd:

1. If you can factor a and b into primes; for each prime number, look at the powers that it appears in the factorization of a and b, take the smaller of the two. Put these prime powers together to get the gcd.

   $576=2^6. 3^2$, $135=3^3.5$, $gcd(576,135)=3^2=9$

   $gcd(2^5. 3^4. 7^2, 2^2. 5^3. 7)= 2^2. 3^0. 5^0. 7^1= 2^2. 7=28$.

Greatest Common Divisor

2. Suppose a and b are large numbers. The gcd can be calculated by using Euclidean Algorithm.

Example: gcd(482, 1180)=?

1180=2.482+216

482=2.216+50

216=4.50+16

50=3.16+**2**

16=8.2+0

Notice that how the numbers are shifted?

The last non-zero remainder is the GCD.
gcd(482, 1180)=2

Greatest Common Divisor

- **Example:**

$$\gcd(12345\ ,\ 11111) = ?$$

$$12345 = 1.11111 + 1234$$

$$11111 = 9.1234 + 5$$

$$1234 = 246.5 + 4$$

$$5 = 1.4 + 1$$

$$4 = 4.1 + 0$$

gcd(12345, 11111)=1

Euclid’s Algorithm and Continued Fraction

- Let a,b,q,r Є Z with b>0 and 0≤r<b such that a=b.q+r then gcd(a,b)=gcd(b,r).
- Proof
  - Let X=gcd(a,b) and Y=gcd(b,r), we should know X=Y
  - If integer c, c|a and c|b, it follows equation a=b.q+r and the divisibility properties that c is a divisor of r also. By the same argument, every common divisor of b and r is a divisor of a.

Greatest Common Divisor

So, the formal description of the Euclidean Algorithm:

Suppose that a>b , if not; switch a and b.

Step 1. divide a by b and represent in the form: $a=q_1b+r_1$

Step 2. If $r_1=0$ then b divides a and gcd is b.

If $r_1\neq0$ then continue by representing b in the form $b=q_2r_1+r_2$

Continue in this way until remainder is zero, giving the following sequence steps:

$$
\begin{aligned}
a &= q_1b + r_1\\
b &= q_2r_1 + r_2\\
r_1 &= q_3r_2 + r_3\\
&\vdots\\
r_{k-2} &= q_kr_{k-1} + r_k\\
r_{k-1} &= q_{k+1}r_k
\end{aligned}
$$

The conclusion is $\gcd(a,b)=r_k$. This algorithm does not require factorization of numbers and it is fast.

Greatest Common Divisor

- Theorem

  Let $a,b \in Z$ with at least one of a, b non-zero, and let $d=\gcd(a,b)$. Then there exist integers x, y such that $ax+by=d$. In particular, if a and b are relatively prime, then there exist integers x, y with $ax+by=1$.

Solving ax+by=d

- We did not use the quotients in the Euclidean Algorithm.

  ax+by=gcd(a,b) ➔ How we find x and y?

$$\gcd(482,1180)=2$$
$$1180=2.482+216$$
$$482=2.216+50$$
$$216=4.50+16$$
$$50=3.16+2$$
$$16=8.2+0$$

The successive quotients be q_1=2, q_2=2, q_3=4, q_4=3 and q_5=8.
From the following sequences:
$x_0=0$, $x_1=1$, $x_j=-q_{j-1}.x_{j-1}+x_{j-2}$
$y_0=1$, $y_1=0$, $y_j=-g_{j-1}.y_{j-1}+y_{j-2}$
Then $ax_n+by_n=\gcd(a,b)$

$$x_0=0; x_1=1$$
$$x_2=-2x_1+x_0=-2$$
$$x_3=-2x_2+x_1=5$$
$$x_4=-4x_3+x_2=-22$$
$$x_5=-3x_4+x_3=71$$

Similarly we calculate y_5=-29.
An easy calculation shows that 482.71+1180.(-29)=2
gcd(482, 1180)=2
Notice that we did not use the final quotient. If we had used it, we would have calculated x_{n+1}=590, which is the 1180/2 and similarly y_{n+1}=241 is 482/2.

This method is called Extended Euclidean Algorithm and it will use for solving congruencies!

Solving ax+by=d

- Example: 22x + 60y = gcd(60,22) find the gcd(60,22) by Euclidean Algorithm.

$$60 = 2.22 + 16$$

gcd(60,22)=2

$$22 = 1.16 + 6$$

$$16 = 2.6 + 4$$

$$6 = 1.4 + 2$$

$$4 = 2.2 + 0$$

$$a = 2.b + 16 \Rightarrow 16 = a - 2b$$

$$b = 1.16 + 6 \Rightarrow 6 = b - 1.16 = b - (a - 2b) = -a + 3b$$

$$16 = 2.6 + 4 \Rightarrow 4 = 16 - 2.6 = (a - 2b) - 2.(-a + 3b) = 3a - 8b$$

$$6 = 1.4 + 2 \Rightarrow 2 = 6 - 4 = (-a + 3b) - (3a - 8b) = -4a + 11b$$

$$-4a + 11b = \gcd(a,b) = 2 = -4.60 + 11.22$$

$$= -240 + 242 = 2$$

Solving ax+by=d

- The equation ax+by=gcd(a,b) always has a solution in integers x and y.
- Question: How many solution it has? And how to describe all of the solutions?
- Let’s start with the case that gcd(a,b)=1, suppose that (x_1,y_1) is a solution to the equation ax+by=1.

  We can find other solutions for any k (kЄZ) as

$$(x_1 + k.b, y_1 - k.a)$$

$$a.(x_1 + k.b) + b(y_1 - k.a) = ax_1 + a.k.b + by_1 - b.k.a = ax_1 + by_1 = 1$$

•Example: $5x + 3y = 1 \Rightarrow (x_1, y_1) = (-1,2)$

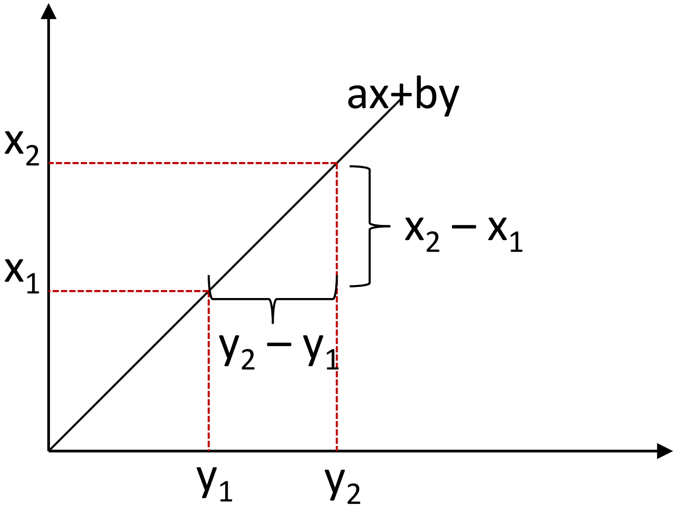
$\ldots$

$for \quad k = -4 \Rightarrow (-13,22)$

$for \quad k = -3 \Rightarrow (-10,17)$

$\ldots$

Solving ax+by=d



If $ax_1+by_1=1$ multiply by y_2 and

$ax_2+by_2=1$ multiply by y_1 and subtract them

$ax_1y_2 – ax_2y_1 =y_2-y_1$

If multiply by x_2 and x_1 and subtract

$bx_2y_1 – bx_1y_2=x_2 – x_1$

So if we let $k=x_2y_1 – x_1y_2$ then we find that

$x_2=x_1+kb$ and $y_2=y_1-ka$.

Geometricaly: if we start the point (x_1,y_1) on the line ax+by=1 and using the fact that the line has slope –a/b to find new points $(x_1+t, y_1 – (a/b)t)$.

t should be multiple of b. Substituting t=k.b gives the new integer solutions

(x_1+kb, y_1-ka).

If gcd(a,b)>1; ax+by=g ➔ (a/g)x+(b/g)y=1 ➔$(x_1+k.(b/g), y_1 – k.(a/g))$ k=0,1,…

Which is called as Linear Equation Theorem.

Congruences

- Definition
  - Let a,b,n Є Z with n≠0, we say that a≡b (mod n), or a is congruent to b mod n.
  - If (a – b) is a multiple (positive or negative) of n.
  - This can be rewritten as a=b+n.k for some integer k.

Examples: $16 \equiv 1 \pmod{5}$

$-3 \equiv 6 \pmod{9}$

$-12 \equiv 2 \pmod{7}$

Congruences

- Propositions: Let a,b,n Є Z with n≠0
  1. $a \equiv 0 \pmod{n}$ iff $n|a$.
  2. $a \equiv a \pmod{n}$ iff $a < n$
  3. $a \equiv b \pmod{n}$ iff $b \equiv a \pmod{n}$
  4. If $a \equiv b$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

  Often we will work integers mod n, denoted Z_n. These may be regarded as the set of {0,1,2,…, n-1} with addition, subtraction and multiplication mod n.

  If a is any integer, we may divide a by n and obtain a remainder in this set $a=n.q+r$ with $0 \le r < n$ then

  $a \equiv r \pmod{n}$.

Congruences

- Propositions: Let $a,b,c,d,n \in \mathbb{Z}$ with $n \neq 0$ and suppose $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

  $a+c \equiv b+d,\ \ a - c \equiv b - d,\ ac \equiv bd \pmod{n}$

  Proof: $a=b+n.k$ and $c=d+n.l$ for $k,l \in \mathbb{Z}$. Then

  $a+c \equiv b+ d + n(k+l)$ so $a+c \equiv b+d \pmod{n}$

Example: Solve $x+7 \equiv 3 \pmod{17}$

$$x \equiv 3 - 7 \equiv -4 \equiv 13 \pmod{17}$$

Congruences

- Division: The general rule is that you can divide by a (mod n) when gcd(a,n)=1.
- Proposition: Let a,b,c,n Є Z with n≠0 and with gcd(a,n)=1.
  - If a.b ≡ a.c (mod n) then b ≡ c (mod n). In other words, if a and n are relatively prime, we can divide both sides of the congruence by a.
- Proof: Since gcd(a,n)=1, there exist integers x, y such that ax+ny=1. Multiply by (b – c) to obtain

  (ab – ac)x + n(b – c)y = b – c

  Since a.b – a.c is a multiple of n, by assumption and n(b – c)y is also a multiple of n, we find that b – c is a multiple of n. This means than b ≡ c (mod n)

Congruences

- Example: Solve 2x+7≡3 (mod 17)

  2x ≡ 3 – 7 ≡ -4 so x ≡ -2 ≡ 15 (mod 17) The division by 2 is allowed since gcd(2, 17)=1.

- Example: Solve 5x +6 ≡ 13 (mod 11)

  5x ≡ 7 (mod 11) ➔ Note that 7 ≡ 18 ≡ 29 ≡ 40≡… (mod 11)

So; 5x ≡ 7 (mod 11) is the same as 5x ≡ 40 (mod 11). Now we can divide by 5 and obtain x ≡ 8 (mod 11).

Note that 7 ≡ 8.5 (mod 11), so 8 acts like 7/5.

Another solution is; since 5.9 ≡ 1 (mod 11). We see that 9 is the multiplicative inverse of 5 (mod 11). Therefore dividing 5 can be accomplished by multiplying by 9.

5 x≡ 7 (mod 11) ➔ x ≡7/5 ≡ 7.9 ≡ 63 ≡ 8 (mod 11)

Congruences

- Proposition: Suppose gcd(a,n)=1. Let s,t Є Z such that a.s+n.t=1 (they can be found by using Extended Euclidean Algorithm). Then a.s≡1 (mod n), so s is the multiplicative inverse for a(mod n).
- Example: 11111.x ≡ 4 (mod 12345)

$$\gcd(12345,11111) = 1 \quad as\ follows$$

$$12345 = 1.11111 + 1234$$

$$11111 = 9.1234 + 5$$

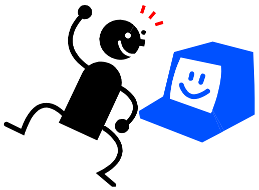
$$1234 = 246.5 + 4$$

$$5 = 1.4 + 1$$

$$4 = 4.1 + 0$$

The successive quotients be q_1=1, q_2=9, q_3=246, q_4=1and q_5=4.
Form the following sequences according to Extended Euclidean Alg
x_0=0, x_1=1, (x_j=-q_{j-1}.x_{j-1}+x_{j-2}) and y_0=1, y_1=0, y_j=-g_{j-1}.y_{j-1}+y_{j-2} Then ax_n+by_n=gcd(a,b)
x_0=0, x_1=1, x_2=-1, x_3=10, x_4=-2461, x_5=2471 which tells us that
11111. 2471 + 12345. y_5= 1 hence 11111.2471 ≡ 1 (mod 12345)
Multipliying both sides of the original congruence by 2471 yields x≡9884 (mod 12345)
In practice means that if we are working mod 12345 and we encounter the fraction 4/11111, we can replace it 9884.

Congruences



- Summary: Finding **a^{-1} (mod n);**

1. Use the **extended Euclidean Algorithm** to find integers s and t such that a.s+n.t=1
2. $a^{-1} \equiv s$ (mod n)

- Solving a.x ≡ c (mod n) when **gcd(a,n)=1**

1. Use the **extended Euclidean Algorithm** to find integer s and t such that a.s+n.t=1.
2. The solution is x≡c.s (mod n)

Congruences

- What if gcd(a,n)>1?
  - Occasionally we will need to solve congruences of the form ax≡b (mod n) when gcd(a,n)=d > 1. The procedure is;

1. If d does not divide b, there is no solution.
2. Assume d|b and consider the new congruence

   (a/d)x ≡(b/d) mod(n/d).

Note that (a/d), (b/d),(n/d) are integers and gcd(a/d,n/d)=1. Solve this congruence by the above procedure to obtain solution x_0.

3. The solution of the original congruence ax≡b (mod n) are x_0, x_0+(n/d) , x_0+2(n/d) , .., x_0+(d-1)(n/d) (mod n)

Congruences

- Example: Solve 12x≡21 (mod 39).

gcd(12,39)=3 which divides 21. Divide by 3 to obtain new congruence 4x ≡7 (mod 13)

$$10.4x \equiv 7.10 (\mathrm{mod} 13)$$

$$x \equiv 70 (\mathrm{mod} 13)$$

$$x_0 \equiv 5 (\mathrm{mod} 13)$$

A solution x_0=5 can be obtained by trying few numbers or by using extended Euclidean Algorithm. The solutions to the original congruence are x≡5, 18, 31 (mod 39)

Fermat’s Little Theorem

- $x^{p-1} \equiv 1\ (mod\ p)$ is FLT
- We can use FLT to simplify computations for large numbers;

$$2^{35} \equiv ?(\mathrm{mod} 7) \Rightarrow 35 \equiv 6.5 + 5 \qquad and$$

$$2^{35} = (2^{6})^{5}.2^{5} \equiv 1^{5}.2^{5} \equiv 32 \equiv 4(\mathrm{mod} 7)$$

EULER’s Phi Function

- $\Phi(m) = the\ order\ of\ the\ relatively\ prime\ numbers\ with\ m$.
- Euler’s formula is; $a^{\Phi(m)} \equiv 1(\mathrm{mod}\, m)$

1. If m=p is prime then every integer 1≤a≤p-1 is relatively prime to m, thus $\Phi(p) = p-1$
2. If $m = p^k \Rightarrow \Phi(p^k) = p^k - p^{k-1}$
3. If $m = p^j.q^k \Rightarrow \Phi(p^j.q^k) = \Phi(p^j).\Phi(q^k)$
4. If $\gcd(m,n) = 1 \Rightarrow \Phi(m.n) = \Phi(m).\Phi(n)$

This is important for composite numbers and simplifying computation for large composite numbers;

If $\gcd(a,m) = 1 \Rightarrow a^{\Phi(m)} \equiv 1(\mathrm{mod}\, m)$

Chinese Remainder Theorem

- Suppose that a number x satisfies x≡25 (mod 42). This means that we can write x=25+42k for some integer k.
- **Rewriting 42 as 7.6** we obtain x=25+7.(6.k), which implies that **x ≡25 ≡4 (mod 7).**
- Similarly, x=25+6.(7.k), which implies that **x ≡25 ≡1 (mod 6).**
- Therefore;

$$x \equiv 25 \pmod{42} \Rightarrow \begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 1 \pmod{6} \end{cases}$$

$[4]_7$	4	11	18	25	32	…
$[1]_6$	1	7	13	19	25	…

The Chinese Remainder Theorem shows that this process can be reversed.

Chinese Remainder Theorem

- Suppose **gcd(m,n)=1** and **a,bЄZ**, there exist exactly one solution **x (mod m.n)** to the simultaneous congruences;

  x ≡ a (mod m)

  x ≡ b (mod n)

- **Proof:** There exist integers **s** and **t**, such that **m.s+n.t=1**.

  Then **m.s ≡ 1 (mod n)** and **n.t ≡1 (mod m)**

  Let **x=b.m.s+a.n.t**

  Then **x ≡a.n.t ≡a (mod m)** and

  x ≡b.m.s ≡b (mod n) so a solution **x** exists.

Suppose **x_1** is another solution.

Then **$x \equiv x_0$ (mod m)** and **$x \equiv x_1$ (mod n)** so **x_0-x_1** is a multiple of both **m** and **n**.

Chinese Remainder Theorem

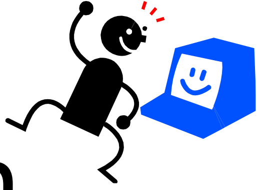
- Lemma: Let m,nЄZ with gcd(m,n)=1. If an integer c is a multiple of both m and n, then c is a multiple of m.n.

Example: solve x ≡3(mod 7), x ≡5(mod 15)

1. 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, ….
2. These numbers are taken by (mod 7) and their congruencies are; 5, 6, 0, 1, 2, 3, 4, … Since we want to find 3 (mod 7) and its matched with 80.

   80 ≡ 3 (mod 7) and 80 ≡5 (mod 15)

- For slightly larger numbers m and n, making a list would be inefficient.



Chinese Remainder Theorem

- The numbers **x ≡b (mod n)** are of the form **x=b+n.k** with kЄZ, so we need to solve **b+n.k≡a (mod m)**.
- This is the same as; **n.k ≡ a – b (mod m)**
- Since **gcd(m,n)=1** by assumption, there is a **multiplicative inverse i for n (mod m).** Multiplication by i gives;

  k ≡ (a – b).i (mod m)

  Substituting back into **x=b+n.k**, then **reducing (mod m.n)** gives the answer.

- **Example:** Solve x ≡7 (mod 12345), x ≡3 (mod 11111)

  The inverse of 11111 (mod 12345) is **i**=2471.

  Therefore k ≡2471.(7 – 3) ≡9884 (mod 12345)

  This yields **x=3+11111.9884** ≡ 109821127 (mod 11111.12345)

Chinese Remainder Theorem

- How do you use the Chinese Remainder Theorem?

  If you start with a congruence **mod a composite number n**, you can break it into simultaneous congruencies 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 congruencies mod primes or mod prime powers than to work mod composite numbers.

Chinese Remainder Theorem General Form

- Let m_1, .., m_k ЄZ with gcd(m_i, m_j)=1 whenever i≠j. Given integer a_1,…,a_k there exist exactly one solution x (mod m_1. … .m_k) to the simultaneous congruencies x≡ a_1 (mod m_1), x ≡ a_2 (mod m_2), …, x ≡ a_k (mod m_k)
- **As a summary for solution x≡ a (mod m), x ≡ b (mod n):**

  1. Find integer **u** and **v** such that **m.u+n.v=1** by using **Euclid's Algorithm.**

  2. Then all solutions are **x ≡ (m.u).b+(n.v).a (mod m.n)**

Chinese Remainder Theorem

Example: x≡ 23 (mod 100), x ≡31 (mod 49)

First we have to solve 100u+49v=1

Euclid’s Algorithm gives;

$x_2=-q_1.x_1+x_0$

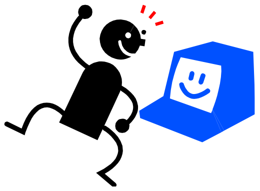
$y_2=-q_1.y_1+y_0$

Divident		Quotient	Divisor		Remainder	v=x	u=y
						0	1
						1	0
100	=	2	49	+	2	-2	1
49	=	24	2	+	1	49	24
2	=	2	1	+	0	-100	49

Then; 49.49 – 24.100=1.

The solution is 49.49.23 – 24.100.31=-19177 ≡ 423 (mod 4900).

Chinese Remainder Theorem



- Remark: If the system of the linear congruences is solvable (if $m_1, m_2, .., m_n$ are pairwise relatively prime and greater than 1) then its solution can be conveniently described as follows;

$$x \equiv \sum_{i=1}^{n} a_i . M_i . M_i^{'} \pmod{m}$$

$$where$$

$$m = m_1 . m_2 ... m_n$$

$$M_i = m / m_i$$

$$M^{'} = M_i^{-1} \pmod{m_i} \quad for \quad i = 1,2,...,n$$

Chinese Remainder Theorem

Example: Consider the following congruencies;

$$x \equiv 2(\mathrm{mod}3)$$
$$x \equiv 3(\mathrm{mod}5)$$
$$x \equiv 2(\mathrm{mod}7)$$

We have;

$$m = m_1.m_2.m_3 = 3.5.7 = 105$$
$$M_1 = m / m_1 = 105/3 = 35$$
$$M_1^{'} = M_1^{-1}(\mathrm{mod}\, m_1) = 35^{-1}(\mathrm{mod}3) = 2$$
$$M_2 = m / m_2 = 105/5 = 21$$
$$M_2^{'} = M_2^{-1}(\mathrm{mod}\, m_2) = 21^{-1}(\mathrm{mod}5) = 1$$
$$M_3 = m / m_3 = 105/7 = 15$$
$$M_3^{'} = M_3^{-1}(\mathrm{mod}\, m_3) = 15^{-1}(\mathrm{mod}7) = 1$$

Hence;

$$x = a_1.M_1.M_1^{'} + a_2.M_2.M_2^{'} + a_3.M_3.M_3^{'} \quad (\mathrm{mod}\, m)$$
$$x = 2.35.2 + 3.21.1 + 2.15.1 \quad (\mathrm{mod}105)$$
$$x = 23$$

Chinese Remainder Theorem

- Example 1
- Solve for largest x such that

$$
\begin{aligned}
x &\equiv 0 \pmod{5} \\
x &\equiv 9 \pmod{11} \\
x &\equiv 10 \pmod{21} \\
x &\leq 2222
\end{aligned}
$$

Chinese Remainder Theorem

- Step 1: $N = 5 \times 11 \times 21 = 1155$
- Step 2: $N_1 = 231, N_2 = 105, N_3 = 55$
- Step 3: $N_1' = 1, N_2' = 2, N_3' = 13$
- Step 4:

$$\begin{aligned} x &\equiv 0 \cdot 1 \cdot 231 + 9 \cdot 2 \cdot 105 + 10 \cdot 13 \cdot 55 \\ &\equiv 9040 \equiv 955 \pmod{1155} \end{aligned}$$

- Step 5:

$$x = 955 + p \times 1155 \leq 2222$$

$$x = 955 + 1155 = 2110$$

Chinese Remainder Theorem

- What if $\exists i, j \text{ s.t. } i \neq j \wedge \gcd(n_i, n_j) \neq 1$?
- We can always reduce them
- Example 2
  - Solve the largest x such that

$$\begin{aligned} x &\equiv 31 \pmod{33} \\ x &\equiv 10 \pmod{105} \\ x &\equiv 20 \pmod{55} \\ x &\leq 2222 \end{aligned}$$

Chinese Remainder Theorem

- Analyze n_i first

$$\begin{aligned} n_1 &= 3 \times 11 \\ n_2 &= 3 \times 5 \times 7 \\ n_3 &= 5 \times 11 \end{aligned}$$

- Thus, we have

$$\begin{aligned} x &\equiv 31 \pmod{33} \\ x &\equiv 10 \pmod{105} \\ x &\equiv 20 \pmod{55} \\ x &\leq 2222 \end{aligned} \iff \begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 0 \pmod{5} \\ x &\equiv 3 \pmod{7} \\ x &\equiv 9 \pmod{11} \\ x &\leq 2222 \end{aligned}$$

Chinese Remainder Theorem

- Take a look at $n_2 = 3 \times 5 \times 7 = 5 \times 21$
- So

$$\begin{array}{lcl} x \equiv 31 \pmod{33} & & x \equiv 0 \pmod{5} \\ x \equiv 10 \pmod{105} & \iff & x \equiv 9 \pmod{11} \\ \multicolumn{3}{c}{\boxed{x \equiv 20 \pmod{55} \qquad\qquad x \equiv 10 \pmod{21}}} \\ x \leq 2222 & & x \leq 2222 \end{array}$$

- Same as example 1
- We want n_is to be relatively prime only!

Fast Modular Exponentiation

Q: How is it even possible to compute 2853^{3397} **mod** 4559 ? After all, 2853^{3397} has approximately 3397·4 digits!

A: By taking the **mod** after each multiplication:

23^3 **mod** 30 $\equiv -7^3 \pmod{30} \equiv (-7)^2 \cdot (-7) \pmod{30}$

$\equiv 49 \cdot (-7) \pmod{30} \equiv 19 \cdot (-7) \pmod{30}$

$\equiv -133 \pmod{30} \equiv 17 \pmod{30}$

Therefore, 23^3 **mod** 30 = 17.

Q: What if had to figure out 23^{16} **mod** 30. Same way tedious: need to multiply 15 times. Is there a better way?

Fast Modular Exponentiation

A: Notice that 16 = $2\cdot2\cdot2\cdot2$ so that

$23^{16} = 23^{2\cdot2\cdot2\cdot2} = (((23^2)^2)^2)^2$

Therefore:

23^{16} **mod** 30 $\equiv (((-7^2)^2)^2)^2 \pmod{30}$

$\equiv (((49)^2)^2)^2 \pmod{30} \equiv (((-11)^2)^2)^2 \pmod{30}$

$\equiv ((121)^2)^2 \pmod{30} \equiv ((1)^2)^2 \pmod{30}$

$\equiv (1)^2 \pmod{30} \equiv 1 \pmod{30}$

Which implies that 23^{16} **mod** 30 = 1.

Q: How about 23^{25} **mod** 30 ?

Fast Modular Exponentiation

A: The previous method of ***repeated squaring*** works for any exponent that's a power of 2. 25 isn't. However, we can break 25 down as a sum of such powers: 25 = 16 + 8 + 1. Apply repeated squaring to each part, and multiply the results together. Previous calculation:

23^8 **mod** 30 = 23^{16} **mod** 30 = 1

Thus: 23^{25} **mod** 30 $\equiv 23^{16+8+1}$ (mod 30) $\equiv$

$23^{16} \cdot 23^{8} \cdot 23^{1}$ (mod 30) $\equiv 1 \cdot 1 \cdot 23$ (mod 30)

Final answer: 23^{25} **mod** 30 = 23

Fast Modular Exponentiation

Q: How could we have figured out the decomposition 25 = 16 + 8 + 1 from the binary (unsigned) representation of 25?

A: $25 = (11001)_2$ This means that

$25 = 1\cdot16+1\cdot8+0\cdot4+0\cdot2+1\cdot1 = 16+8+1$

Can tell which powers of 2 appear by where the 1's are. This follows from the definition of binary representation.

How do you compute…

$5^{121242653}$ (mod 11)

The current best idea would still need about 54 calculations

answer = 4

Can we exponentiate any faster?

OK, need a little more number theory for this one…

First, recall…

$Z_n = \{0, 1, 2, \ldots, n-1\}$

$Z_n^* = \{x \in Z_n \mid GCD(x,n) = 1\}$

Fundamental lemmas mod n:

If ($x \equiv_n y$) and ($a \equiv_n b$). Then

1) $x + a \equiv_n y + b$
2) $x * a \equiv_n y * b$
3) $x - a \equiv_n y – b$
4) $cx \equiv_n cy \Longrightarrow a \equiv_n b$

i.e., if c in Z_n^*

Euler Phi Function Á(n)

Á(n) = size of Z_n^*

p prime ⇒ Á(p) = p-1

p, q distinct primes ⇒
Á(pq) = (p-1)(q-1)

~~Fundamental lemma of powers?~~

If $(x \equiv_n y)$
Then $a^x \equiv_n a^y$?

NO!

$(2 \equiv_3 5)$, but it is not the case that: $2^2 \equiv_3 2^5$

(Correct) Fundamental lemma of powers.

If $a \in Z_n^*$ and $x \equiv_{\text{Á}(n)} y$ then $a^x \equiv_n a^y$

Equivalently,

for $a \in Z_n^*$, $a^x \equiv_n a^{x \bmod \text{Á}(n)}$

How do you compute…

$5^{121242653}$ (mod 11)

121242653 (mod 10) = 3

5^3 (mod 11) = 125 mod 11 = 4

Why did we
take mod 10?

for a $\in Z_n^*$, $a^x \equiv_n a^{x \bmod \text{Á}(n)}$

Hence, we can compute
a^m (mod n)
while performing at most
$2\lfloor \log_2 \text{Á}(n) \rfloor$ multiplies

where each time we multiply
together numbers
with $\lfloor \text{log2 } n \rfloor + 1$ bits

$343281^{327847324}$ mod 39

Step 1: reduce the base mod 39 ; $343281 \equiv 3 \; mod \; 39$

Step 2: reduce the exponent mod Á(39) = (3-1)(13-1)=2.12=24;

$$327847324 \equiv 4$$

NB: you should check that gcd(343280,39)=1 to use lemma of powers

Step 3: use repeated squaring to compute 3^4,

taking mods at each step

(Correct) Fundamental lemma of powers.

If $a \in Z_n{}^*$ and $x \equiv_{\Phi(n)} y$ then $a^x \equiv_n a^y$

Equivalently,

for $a \in Z_n{}^*$, $a^x \equiv_n a^{x \bmod \Phi(n)}$

How do you prove the lemma for powers?

Use Euler’s Theorem

For $a \in Z_n^*$, $a^{\Phi(n)} \equiv_n 1$

Corollary: Fermat’s Little Theorem

For p prime, $a \in Z_p^* \Rightarrow a^{p-1} \equiv_p 1$

Proof of Euler's Theorem: for $a \in Z_n^*$, $a^{\Phi(n)} \equiv_n 1$

Define $a Z_n^* = \{a *_n x \mid x \in Z_n^*\}$ for $a \in Z_n^*$

By the cancellation property, $Z_n^* = aZ_n^*$

$\prod x \equiv_n \prod ax$ [as x ranges over Z_n^*]

$\Pi\, x \equiv_n \prod x\ (a^{\text{size of } Zn^*})$ [Commutativity]

$1 =_n a^{\text{size of } Zn^*}$ [Cancellation]

$a^{\Phi(n)} =_n 1$

Please remember

Euler's Theorem

For $a \in Z_n^*$, $a^{\Phi(n)} \equiv_n 1$

Corollary: Fermat's Little Theorem

For p prime, $a \in Z_p^* \Rightarrow a^{p-1} \equiv_p 1$

Primality Test

- Step 1: Pick a random number a, set $k = n - 1$
- Step 2: Calculate $a^k \bmod n$

Check when k < n - 1

- Step 3: If not 1 (and not -1), composite, done
- Step 4: If -1, “probably” prime, done
- Step 5: If 1 and k is odd, “probably” prime, done
- Step 6: $k := \frac{k}{2}$, go back to step 2

Primality Test

- Example: Test if n=221 is prime and k=220
- Pick a=174 to test

$$174^{220} \bmod 221 = 1$$
$$174^{110} \bmod 221 = 220$$

- Under this test, 221 is “probably” prime
- Pick 137 to test

$$137^{220} \bmod 221 = 35$$

- We are sure 221 is composite!
- 174: strong liar, 137: witness

Deterministic or Non-Deterministic algorithms for Primality Testing

- Deterministic algorithms
  - The AKS primality testing
  - The Sieve of Eratosthenes
  - The Lucas–Lehmer–Riesel test
- Non-Deterministic algorithms
  - Fermat’s little theorem
  - Solovay-Strassen primality test
  - Miller-Rabin primality test
  - Chinese hypothesis
  - Elliptic Curve primality test

The End