Recall $n \in \mathbb{N}$

$\mathbb{Z}/n\mathbb{Z} = \{0,1,2,\dots,n-1\}$

$a,b \in \mathbb{Z}$

$a+b \equiv r \mod m$

HW #6 r unique $\ni$ $0 \le r < m$ s.t. $(a+b)-r$ divisible by m

$\overline{r} = \overline{a+b}$

$\overline{a}\cdot\overline{b} := \overline{ab}$

Ex/ $\mathbb{Z}/6\mathbb{Z} = \{\bar 0,\bar 1,\bar 2,\bar 3,\bar 4,\bar 5\}$

$\bar 5 \cdot \bar 3 = \overline{15} = \bar 3$

$\bar 2 \cdot \bar 3 = \bar 6 \equiv 0 \mod 6$

In $\mathbb{Z}/m\mathbb{Z}$ can $+$, can $\times$, can $-$

When can we divide?

A. $a \in \mathbb{Z}/m\mathbb{Z}$ has an inverse $\Leftrightarrow \gcd(a,m)=1$

Pf/ Extended Euc. Alg. $\varnothing$

Def^n $m \in \mathbb{N}$ The group of units of $\mathbb{Z}/m\mathbb{Z}$ is

$(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(a,m)=1\}$

Claim/ $a,b \in (\mathbb{Z}/m\mathbb{Z})^*$ $\Rightarrow ab \in (\mathbb{Z}/m\mathbb{Z})^*$

Pf/ Show $\exists\ (ab)^{-1}$

w/ a^{-1} exists, b^{-1} exists

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$
$\equiv a(1)a^{-1} \mod m$
$\equiv 1 \mod m$

$\Rightarrow \gcd(ab,m)=1$

$\Rightarrow ab \in (\mathbb{Z}/m\mathbb{Z})^*$

$\varnothing$

Example

- 0 never in $(\mathbb{Z}/m\mathbb{Z})^*$
- $(\mathbb{Z}/24\mathbb{Z})^* = \{1,5,7,11,13,17,19,23\}$
- $(\mathbb{Z}/7\mathbb{Z})^* = \{1,2,3,4,5,6\}$

Def^n Euler ϕ-function

$\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^*$

Ex $\phi(24)=8$
$\phi(7)=6$

Warning

$(\mathbb{Z}/m\mathbb{Z})^*$ does not have addition.

Ex $5,7 \in (\mathbb{Z}/24\mathbb{Z})^*$

$(5+7=12 \quad \gcd(12,24)=12)$
$12 \notin (\mathbb{Z}/24\mathbb{Z})^*$

$5\cdot 7 = 35 \equiv 11 \mod 24$

Fast Powering

In RSA (& more) need to compute $g^A \mod N$
$g \in \mathbb{Z}/N\mathbb{Z}$, $N \in \mathbb{N}$, $A \in \mathbb{N}$

How?

$g^A = \overbrace{g\cdot g\cdot g \cdots g}^{A \text{ times}} \mod N$

Problem: A might be huge.

g^A = HUGE

Instead Reduce mod N @ each step.

HW #8

$g_1 \equiv g$

$g_2 \equiv g_1 \cdot g \mod N$

$g_3 \equiv g_2 \cdot g$
$\equiv (g_1\cdot g)\cdot g$
$\equiv g^3 \mod N$

$\vdots$

$g_A \equiv g_{A-1}\cdot g \mod N$

$g_A \equiv g^A \mod N$

Bad news Takes A multiply & reduce steps.

If $A \sim 2^{1000}$

Takes > age of universe.

Example (1.18)

$3^{218} \mod 1000$

Step 1: Binary Expand 218

$218 = 128+64+16+8+2$
$= 2^7+2^6+2^4+2^3+2^1$

$$\begin{array}{r} 218 \\ -128 \\ \hline 90 \\ -64 \\ \hline 26 \\ -16 \\ \hline 10 \\ -8 \\ \hline 2 \\ -2 \\ \hline 0 \end{array}$$

11011010

Therefore

$3^{218} = 3^{2^1+2^3+2^4+2^6+2^7}$
$= 3^{2^1}\cdot 3^{2^3}\cdot 3^{2^4}\cdot 3^{2^6}\cdot 3^{2^7}$

Step 2 Compute $3^{2^7} \mod 1000$ by squaring 3, 7 times

i	0	1	2	3	4	5	6	7
3^{2^i}	3	9	81	561	721	841	281	961

$3^{2^2} = (3^2)^2 = 9^2 = 81$

$3^{2^3} = (3^{2^2})^2 = 81^2 = 6561$
$\equiv 561 \mod 1000$

$3^{2^4} = (3^{2^3})^2 \equiv (561)^2 \mod 1000$
$= 314721 \equiv 721$

Step 3: Substitute & multiply

$3^{218} = 3^{2^1}\cdot 3^{2^3}\cdot 3^{2^4}\cdot 3^{2^6}\cdot 3^{2^7}$
$\equiv 9(561)(721)(281)(961) \mod 1000$

$\equiv (5049)(721)(281)(961)$
reduce

$\equiv 49(721)(281)(961) \mod 1000$

$\equiv \cdots$

$\equiv 489 \mod 1000.$

Time Analysis

$\varnothing$ Naive Way
218 multiplications

$\varnothing$ Fast Powering
- square & reduce $\times 7$
- Multiply & reduce $\times 4$

$\Rightarrow$ 11 steps.

Fast Powering Alg.

Inputs: $N \in \mathbb{N}$, $g \in \mathbb{Z}/N\mathbb{Z}$, $A \in \mathbb{N}$

Goal $g^A \mod N$.

Step 1

$A = A_0 + A_1\cdot 2 + A_2 \cdot 2^2 + \dots + A_r \cdot 2^r$

w/ $A_i = 0$ or 1

& $A_r = 1$

Step 2 Compute $g^{2^i} \mod N$ by successively squaring

$a_0 = g$

$a_1 \equiv g^2 \mod N$

$a_2 \equiv a_1^2 \mod N$
$\equiv (g^2)^2 = g^{2^2}$

$a_3 \equiv a_2^2 \mod N$
$\equiv (g^{2^2})^2 = g^{2^3}$

$\vdots$

$a_r = a_{r-1}^2 \mod N$
$\equiv g^{2^r} \mod N$

square r times

Step 3 Compute $g^A \mod N$ by the eqn

Pf/ correct + HW1 #8

$g^A = g^{A_0+A_1\cdot 2+\dots+A_r 2^r}$

$= g^{A_0}\cdot g^{A_1 2^1}\cdots g^{A_r 2^r}$

$= a_0^{A_0}\cdot a_1^{A_1}\cdots a_r^{A_r}$

by multiplying & reducing $\le r$ times

$a_i^{A_i} = \begin{cases} a_i & A_i = 1 \\ 1 & A_i = 0 \end{cases}$

Time Assume binary expansion is fast

At most $2r = 2\log_2 A$ multiplications

$r = \max\{i \mid 2^i \le A\} \le \log_2 A$

E.g. $A \sim 2^{1000}$

Naive: Absurd

F.P. $\le 2\log_2 2^{1000}$
$= 2000$

HW Implement Both naive & fast algorithms.

Finite Fields

- in $\mathbb{Z}/m\mathbb{Z}$ division by a only makes sense if $\gcd(a,m)=1$
- If m = prime then $\forall\ a$ $0<a<m$, $\gcd(a,m)=1$
  $\Rightarrow (\mathbb{Z}/m\mathbb{Z})^* = \{1,2,\dots,m-1\}$

For us care about $\mathbb{Z}/p\mathbb{Z}$ p prime.

can divide by anything except 0.

Def^n $p \in \mathbb{N}$ is prime if $p \ge 2$ & the only divisors >1 of p are 1 & p.

Important property of primeness

Prop: p a prime. $a,b \in \mathbb{Z}$. $p \mid ab$. Then $p \mid a$ or $p \mid b$.

Pf/ $g = \gcd(a,p)$

$\Rightarrow g \mid p \Rightarrow g=1$ or p.

If $g=p \Rightarrow p=g \mid a$
$\Rightarrow$ done.

Extended Euc. Alg
$\exists\ u,v \in \mathbb{Z}$
& $au+pv=1$

$abu+pbv=b$

$p \mid ab \Rightarrow p \mid abu$

$p \mid pbv \Rightarrow p \mid (abu+pbv) = b$ ✓

$\varnothing$

Ex Impt that p prime.
$6 \mid 9\cdot 2$ but $6 \nmid 9$
$6 \nmid 2$

Corollary

p prime. $a_1,\dots,a_n \in \mathbb{Z}$

if $p \mid a_1 a_2 \cdots a_n$

then $p \mid a_i$ some i

Pf/ $p \mid a_1(a_2\cdots a_n)$

$p \mid a_1$ or $p \mid a_2(a_3\cdots a_n)$

done $\Rightarrow p \mid a_2$ or $p \mid a_3(a_4\cdots a_n)$

$\varnothing$ $\vdots$

Theorem (Fundamental theorem of arithmetic)

$a \ge 2$. Then a factors as a primes uniquely up to reordering.

Pf/ Existence

Find smallest prime dividing a. Factor it out. repeat.

Uniqueness

$a = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_r$ $\quad r \ge t$

$p_1 \mid a = q_1 \cdots q_r$ so $p_1 \mid q_i$

reordering $p_1 \mid q_1$
$p_1 = q_1$

$p_2 \cdots p_t = q_2 \cdots q_r$ repeat

$p_2 = q_2$ $\cdots$

$\vdots$

$1 = q_{t+1} \cdots q_r$
$\neq 1$

So $t=r$ & primes agree. $\varnothing$

$\mathbb{Z}/6\mathbb{Z}$

$\mathbb{Z}/6\mathbb{Z}$

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$5 \cdot 5 = 25 \equiv 1 \mod 6$

$(\mathbb{Z}/6\mathbb{Z})^* = \{1, 5\}$

$5 \equiv -1 \mod 6$

Exercise

suppose $a \equiv -1 \mod m$
Show you can divide by a in $\mathbb{Z}/m\mathbb{Z}$.