CIS 700 Lecture 7: Primes

Thm (Fundamental Theorem of Arithmetic)

Every $n \in \mathbb{Z}$ $n \neq 0$ has unique factorization $n = \pm p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

p_i distinct primes, e_i pos. integers

Thm (Division w/ remainder)

$a, b \in \mathbb{Z}$ $b > 0$ $\exists$ unique $q, r \in \mathbb{Z}$ s.t. $a = bq + r$ $0 \leq r < b$

Pf - Existence: Consider $\{ r_t = a - bt \mid t \in \mathbb{Z}, r_t \geq 0 \}$

- nonempty: $a \geq 0$ set $t = 0$, $a < 0$ set $t = a$

Choose smallest r: - $r = a - bq$ for $q \in \mathbb{Z}$

- $r < b$, else $r - b < r$

- Uniqueness: $a = bq + r = bq' + r'$ $0 \leq r < b$ $0 \leq r' < b$

$r' - r = b(q - q')$

$r' - r = bz$ but $|r' - r| < b \Rightarrow r' - r = 0$

$\Rightarrow 0 = b(q - q')$ $b \neq 0 \Rightarrow q - q' = 0$

$a \bmod b = r$ $\qquad$ $a \bmod b = a - b \lfloor \frac{a}{b} \rfloor$

$b \mid a \iff a \bmod b = 0$

$a = b \bmod N$: $(a \bmod N) = (b \bmod N)$

$a = b \bmod N \iff N \mid (a - b)$

$\gcd(a, b)$ = greatest common divisor d $d \mid a, d \mid b$

Thm (Extend Euclidean Alg.)

$a, b \in \mathbb{Z}$ (at positive) $\exists$ $x, y \in \mathbb{Z}$ s.t. $ax + by = \gcd(a, b)$

Pf Let $I = \{ sa + rb \mid r, s \in \mathbb{Z} \}$ Let d smallest pos. elt. of I.

- $d \mid$ every elt. of I: Choose $c = s_c a + r_c b$.

$c = qd + r$: $r = c - qd = s_c a + r_c b - q(ax + by) = (s_c - qx)a + (r_c - qy)b \in I$

$r = 0$ by minimality of d.

$\Rightarrow d \mid c$

- d is largest: Assume $\exists d' > d$ s.t. $d' \mid a, d' \mid b \Rightarrow d' \mid xa + yb \Rightarrow d' \mid d$ but $d' > d \Rightarrow$ contrad.

Math version:

I is an ideal of $\mathbb{Z}$. $I \subseteq \mathbb{Z}$

- closed under addition: $a, b \in I \Rightarrow a+b \in I$
- closed under multiplication in $\mathbb{Z}$: $a \in I, z \in \mathbb{Z} \Rightarrow az \in I$

Facts:

$0 \in I$: $0 \cdot a = 0 \in I$

$a \in I \Rightarrow -a \in I$: $a \cdot (-1) = -a \in I$

$a, b \in I \Rightarrow a - b \in I$

$\{0\}$ is an ideal

$\mathbb{Z}$ is an ideal

$1 \in I \Rightarrow I = \mathbb{Z}$

$a\mathbb{Z} = \{az \mid z \in \mathbb{Z}\}$ = "ideal generated by a"

"principal ideal": ideal of form $a\mathbb{Z}$

Thm All ideals of $\mathbb{Z}$ are principal.

($a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, $d = \gcd(a,b)$)

Extended Euclidean Algorithm

Input: $a, b \in \mathbb{Z}$ $a \geq b > 0$

Output: d, x, y s.t. $d = \gcd(a,b)$ $ax + by = d$

```
If b | a:
    return b, 0, 1
else:
    compute a = q b + r
    d, x, y = egcd(b, r)      (xb + yr = d)
    return (d, y, x - yq)
```

Euclidean Algorithm

```
If b = 0:
    return a
else:
    return gcd(b, a mod b)
```

Thm Extended Euclid Alg. runs in time $O(\lg(a)\lg(b))$

Thm If $c \mid ab$, $\gcd(a,b) = 1 \Rightarrow c \mid b$

Modular inverses:

inverse of b mod N: $bb^{-1} \equiv 1 \bmod N$

Not defined if b not invertible. 0 has no inverse.

Thm a invertible mod $N \iff \gcd(a,N) = 1$.

Pf $\Rightarrow$ $ab \equiv 1 \bmod N$

$ab = 1 + cN$

$ab - cN = 1 \Rightarrow \gcd(a,N) = 1$

$\Leftarrow$ $ax + Ny = 1$

$\Rightarrow x = a^{-1} \bmod N$

Group: $(S, \circ)$

set, operation

G is a group if

- closed under op.
- identity: $\exists\, e \in G$ s.t. $e \circ g = g = g \circ e \ \forall g \in G$
- inverses: $\forall g \in G \ \exists h \in G$ s.t. $g \circ h = e = h \circ g$
- associative: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$

abelian group:

- commutative: $\forall g, h \ \ g \circ h = h \circ g$

cyclic group:

$G = (\langle a \rangle, \circ)$

generated by one element

Examples:

$\mathbb{Z}$ abelian group w/ $+$: identity $= 0$, inverse: $-g$ cyclic, generated by 1

$\mathbb{Z}$ not group w/ $\times$

$(\mathbb{Z} \bmod N, +)$ is a group cyclic, generated by 1

$(\mathbb{Z} \bmod N, \times)$ not a group

$(\{1, 2, \ldots, p-1\} \bmod p, \times)$ a group, p prime "multiplicative group mod p" $\mathbb{Z}_p^*$

order $p-1$

$|G|$ = "order of group" = # elts

$g^m = \underbrace{g \cdot g \cdot g \cdots}_{m \text{ times}}$

Thm G abelian group w/ $|G| = m \Rightarrow g^m = 1$

Pf $g_1 \cdot g_2 \cdots g_m = (gg_1)(gg_2) \cdots (gg_m) = g^m (g_1 g_2 \cdots g_m)$

Multiply by g for all elts

Cor Let G a group $|G|=m$. If $\gcd(e,m)=1$, $f_e: g \to g^e$ is a bijection.
$d = e^{-1} \bmod m$ $f_d: g \to g^d$ is inverse of f_e

Cor p prime $a^{p-1} \equiv 1 \bmod p$ (Fermat's Theorem)

Idea: Primality testing?

Algorithm: (Cheap primality testing)
Input: N
Output: N prime or composite

1. Choose (random?) a (e.g. $a=2$)
2. Check if $a^{N-1} \equiv 1 \bmod N$
   if yes output "prime"

Thm If $\exists$ witness N is composite (a s.t. $a^{N-1} \not\equiv 1 \bmod N$) $\Rightarrow$ $\frac{1}{2}$ elts. of $\mathbb{Z}_N^*$ are witnesses.

Problem $\exists N$ with no witnesses (Carmichael Numbers)

Miller-Rabin primality test: Fix above for all integers

$\mathbb{Z}_p^*$: Cyclic group of order $p-1$
$\Rightarrow \exists a$ s.t. $G = \langle a \rangle = \{a, a^2, a^3, \ldots, a^{p-1}\}$

Problem: Not every a generates G.
Thm: Order $\langle a \rangle \mid p-1$ (Lagrange)
$\exists$ efficient p.p.t alg. to find generator if factorization of $p-1$ known.

Efficient exponentiation:
$g^a = \underbrace{g \cdot g \cdot g \cdots g}_{a \text{ times}}$ not poly-time in $\log a$

Square and multiply: (left-to-right)
Input base b, exponent a, modulus m
Output: $b^a \bmod m$

```
result = 1
for i = ℓ ... 0: (a has ℓ bits):
    result = result^2 mod m
    if a[i] = 1: (bit i of a is 1)
        result = result · b mod m
return result
```