# Number Theory

A bit more depth...

- modular arithmetic

- primes

- Euclid's algorithm

- Chinese remainder theorem

- Euler's totient function

- Euler's theorem

**Slide 1**

# Modular Arithmetic

- $m, n$ integers, $n > 0$

- remainder of $m/n$: smallest non-negative integer that differs from $m$ by a multiple of $n$: $m = a \cdot n + r$

- C: `-7 % 10 = -7`

- example: 3, 13, -7, 23 have remainder 3 (/10)

- equivalent if same remainder

- usually use smallest positive to represent

- addition:
$$(a + kn) + (b + ln) = (a + b) + (k + l)n = a + b$$

- multiplication:
$$(a + kn)(b + ln) = ab + (al + kb + kln)n$$

**Slide 2**

# Primes

- divisible only by itself and 1

- infinite number

- if finite: multiply them together, add 1

- not divisible by any of them!

- thin out $1/\ln$

**Slide 3**

# Euclid's Algorithm

- find gcd, multiplicative inverses $\mathrm{mod}\,n$

- gcd of two integers = largest integer that divides both

- relatively prime if $\gcd(x, y)$ is 1

- $\gcd(12, 8) = 4, \gcd(12, 25) = 1, \gcd(12, 24) = 12$

- $\gcd(0, x) = x$

- Euclid: replace $x, y$ with smaller numbers until $x$ or $y = 0$

**Slide 4**

## Euclid's Algorithm

- $\gcd(x, y) = \gcd(x - y, y)$ (also divisors)

- if $d$ divides $x, y \Rrightarrow y = kd, x = jd \Rrightarrow x - y = jd - kd = (j - k)d$

- if $d$ divides $x, x - y \Rrightarrow y = kd, x - y = ld \Rrightarrow x = (k + l)d$

- subtract $ny < x \Rrightarrow$ replace with remainder divided by $y$

- switch $x, y$ if $x < y$:
$$\langle x, y \rangle \to \langle y, x \% y \rangle$$

- example: $\gcd(408, 595)$

| $x/y$ | quotient | remainder |
|---|---|---|
| 595/408 | 1 | 187 |
| 408/187 | 2 | 34 |
| 187/34 | 5 | 17 |
| 34/17 | 2 | 0 |

$\Rrightarrow \gcd(408, 595) = 17$

**Slide 5**

## Euclid's Algorithm

- also: $\gcd(x, y) = ux + vy$ (e.g., $\gcd(408, 595) = 17 = -16 \cdot 408 + 11 \cdot 595$)

- if $u' = u + n \Rrightarrow$ multiple of gcd (since $x$ is)

- thus, $x, y$ rp iff $\exists u, v : ux + vy = 1(pmodn)$

**Slide 6**

# Euclid's Algorithm

| $n$ | $q_n$ | $r_n$ | $u_n$ | $v_n$ |
|-----|-------|-------|-------|-------|
| $-2$ | | $x$ | $1$ | $0$ |
| $-1$ | | $y$ | $0$ | $1$ |
| $n$ | $\lfloor r_{n-2}/r_{n-1} \rfloor$ | $r_{n-2} \% r_{n-1}$ | $u_{n-2} - q_n u_{n-1}$ | $v_{n-2} - q_n v_{n-1}$ |

$$
\begin{aligned}
r_n &= r_{n-2} - q_n r_{n-1}; r_0 = x - q_0 y \\
&= u_{n-2}x - v_{n-2}y - q_n(u_{n-1}x + v_{n-1}y) \\
&= (u_{n-2} - q_n u_{n-1})x + (v_{n-2} - q_n v_{n-1})y \\
&= u_n x + v_n y
\end{aligned}
$$

**Slide 7**

# Euclid's Algorithm

| $n$ | $q_n$ | $r_n$ | $u_n$ | $v_n$ |
|-----|-------|-------|-------|-------|
| $-2$ | | $408$ | $1$ | $0$ |
| $-1$ | | $595$ | $0$ | $1$ |
| $0$ | $0$ | $408$ | $1$ | $0$ |
| $1$ | $1$ | $187$ | $-1$ | $1$ |
| $2$ | $2$ | $34$ | $3$ | $-2$ |
| $3$ | $5$ | $17$ | $-16$ | $11$ |
| $4$ | $2$ | $0$ | $35$ | $-24$ |

**Slide 8**

# Finding Multiplicative Inverses

- multiplicative inverse of $m \bmod n$ ➠ $um = 1 \pmod{n}$

- or $um + vn = 1$ for some $v$

- use Euclid's algorithm for $\gcd(m, n)$ to find $u, v$

- unique $u$: assume another $x$ ➠ $xm = 1 \pmod{n}$

- $xmu = u \pmod{n}$ ➠ $x = u \bmod n$

**Slide 9**

# Chinese Remainder Theorem

**Theorem 1** *If $z_1, z_2, \ldots, z_k$ are rp, and if $y = x_k \bmod z_k \forall k$, then one can compute $y \bmod z_1 \cdots z_k$. If $y = x \bmod z_1 \cdots z_k$, one can compute $y \bmod z_1$, etc.*

➠ two representations

**standard:** $x \bmod z_1 \cdots z_k$

**decomposed:** $\langle x_1 \bmod z_1, \ldots \rangle$

decomposed $(x_1 \bmod p, x_2 \bmod q) \rightarrow$ standard $x \bmod pq$

- find $u, v$ such that $up + vq = 1$ (Euclid)

- $x = x_1 + kp$, $x = x_2 + lq$

- $x = upx + vqx$ ➠ $x \bmod pq = (x_2 + lq)up + (x_1 + kp)vq \bmod pq$

- $x = x_2 up + x_1 vq \bmod pq$

**Slide 10**

# CRT Example

- $p = 7, q = 9$

- $50 \bmod pq = 50 \bmod 63 = (1 \bmod 7, 5 \bmod 9)$

- find $u, v$ for $up + vq = 1$

- here: $4 \cdot 7 + (-3) \cdot 9 = 1$

- $x = x_2 up + x_1 bq = 5 \cdot 4 \cdot 7 + 1(-3)9 = 113 = 50 \bmod 63$

**Slide 11**

## $Z_n^*$

- $Z_n$ integers mod $n$

- $Z_n^* =$ relatively prime to $n$

- $Z_{10}^* = \{1, 3, 7, 9\}$

**Theorem 2** *$Z_n^*$ is closed under multiplication* $\bmod n$.

Proof:

- if $a, b \in Z_n^* \implies \exists u_a, v_a, u_b, v_b$ such that $u_a a + v_a n = 1$ and $u_b b + v_b n = 1$

- $(u_a u_b)ab + (u_a v_b a + v_a u_b b + v_a v_b n)n = 1$

- $\implies ab \in Z_n^*$

**Slide 12**

# Euler's Totient Function

- $\phi(n)$ = number of elements in $Z_n^*$

- $\phi(p^\alpha)$, with $p$ prime, $\alpha > 0$

  - only multiples of $p$ are *not* rp to $p^\alpha$

  - ➥ every $p$th number

  - ➥ $p^{\alpha-1}$ not qualified

  - ➥ $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = (p-1)p^{\alpha-1}$

- $\phi(pq)$ ➥ Chinese Remainder Theorem

**Slide 13**

# Euler's Theorem

**Theorem 3** $\forall a \in Z_n^*, a^{\phi(n)} = 1 \bmod n$

Proof:

- multiply all $\phi(n)$ elements of $Z_n^* \to x \in Z_n^*$

- $x$ has inverse $x^{-1}$

- product of all elements $\times a$ ➥ $a^{\phi(n)}x$

- multiplication by $a$ = rearrangement of entries

- $\phi(n)$ rearrangements ➥ $a^{\phi(n)}x = x$

- multiply by $x^{-1}$ ➥ result

**Slide 14**

## Euler's Theorem, Variant

**Theorem 4** $\forall a \in Z_n^*$, $a^{k\phi(n)+1} = a \mod n$

Proof:
$$a^{k\phi(n)+1} = a^{k\phi(n)}a = a^{\phi(n)k}a = 1^k a = a$$

if $k \geq 0$ true also for $a$ not rp $n$ ➠ message $a$ for $n = p \cdot q$

**Slide 15**