NUMBER THEORY: QUICK REFERENCE

VISHVAS VASUKI

Contents

Part 1. Notation

[n]: Set of first n natural numbers.

Part 2. Themes

About Z.

Part 3. Rigorous patterns of ideas and solution strategies

1. Properties of Numbers

Evenness and odness. Primes and composites. Unique factorization of n as product of primes: $n = p_1^{e_1}...$

2. GCD

gcd(x,y). $gcd(x, y)|x - y$.

2.1. Euclid's algorithm. To find gcd(x, y): if $y|x$ return y else return gcd(x, y-x).

From Euclid's alg, GCD(x,y)=ax+by. If 1 = ax+by, a ≡ multiplicative inverse of x mod y.

2.2. Extended Euclid's alg. Find a,b using Euclid's alg.

2.3. Diophontine equation. Indeterminate polynomial eqn with integer solutions: eg: gcd(x, y) = ax + by in Euclid's alg.

3. Conjectures

Goldbach conjecture: $\forall x \in N, x > 4$, x = sum of 2 primes.

4. Primes

4.1. Special primes. Marsenne prime: writ as $2^n - 1$.

4.2. Prime number theorem. Num of primes under k = $\Pi(k) = (1 + o(1))\frac{k}{\ln k}$. [**Find proof**]

(Green, Tao) Number of arithmatic progressions of primes of length $\geq k$ is ≥ 1.

4.3. Primality testing of n. Don't try to factor: assumed hard.

4.4. Randomized primality test. (Miller Rabin) Pick rand x in $Z_n^+ - \{0\}$. If $x|n$ reject. See if (Fermat's little th, Lucas-Lehmer) $\forall x \in Z_n^* : x^{n-1} = 1 \mod n$ holds: do it in polylog time with repeated squaring. Repeat test with many x's. In failure, reject. Else, check if it is a Carmichael composite number: see if 1 has a non-trivial square root: Write $n - 1 = 2^s d$; pick $x \neq \pm 1$; repeatedly square and check if $x \mod n = 1$: if so reject, else if $x \mod n = -1$: try starting with another x.

4.5. Picking some prime below N. Pick a random number below n, check if it is a prime: if not prime fail. By Prime number th, this alg has $\approx (\ln n)^{-1}$ success rate, which can then be amplified.

5. Special numbers

5.1. **Square free integers.** Aka quadratfrei. Divisible by no perfect square except 1.

5.2. **Carmichael composite number.** Let prime factorization: $n = p_1^{e_1}...$ Aka Fermat pseudoprimes: They're Fermat liers: $\forall a: a^{n-1} \equiv 1 \mod n$. n is Carmichael iff it is square free; for all p_i $p_i - 1|n-1$. [**Find proof**]Eg: 561 = 3*11*17; $\forall a: a^{560} = 1 \mod 3, \mod 17, \mod 11$ as $2, 10, 16|560$.

6. Modulo arithmatic

The remainder fn. $-3 \equiv 2 \mod 5$. $ab \mod n \equiv (a \mod n)(b \mod n) \mod n$. So, congruence relation over $\mathbb{Z}$ wrt +, *. If $a \equiv b \mod n \implies n|a-b$.

6.1. **Cancellation law.** $ka \equiv kb \mod n \implies k(a-b) \equiv 0 \mod p \implies a \equiv b \mod n$.

6.2. **Chinese remainder theorem.** Let n_i's coprime, $N = \prod_j n_j$. System of simultaneous congruences $x = a_i \mod n_i$ for $i = 1 \ldots k$ has a unique solution for x in $\mathbb{Z}_N$.

6.2.1. *Uniqueness.* If $\forall i, x \equiv x_i \mod n_i$, and $y \equiv x_i \mod n_i$, $x - y \equiv 0 \mod N$.

6.2.2. *Solving for x.* Use Extended Euclid's alg on $1 = r_i n_i + s_i \frac{N}{n_i}$ to find r_i and s_i, let $e_i = s_i \frac{N}{n_i}$; then $e_i \equiv 1 \mod n_i$ but $0 \mod n_j$; thence find $x = \sum_{i=1}^k a_i e_i$.

6.2.3. *Equivalent statements and implications.* $|Z_N| \to |\times_i Z_{n_i}|$. Map $x \to (x \mod n_1, ..)$ from $Z_N \to \times_i Z_{n_i}$ is both one to one and onto. Also, Isomorphism by Chinese remainder fn: $\mathbb{Z}_n \cong \times_i \mathbb{Z}_{n_i}$ preserves +, *.

6.2.4. *Utility.* Useful for manipulating composite numbers. An airthmatic question mod N reduced to arithmatic questions modulo n_i, if we know $\{n_i\}$.

7. Additive group: Z_p^+

A prime order group. Does not have any subgroups.

8. Multiplicative group Z_N^*

Z_N^* : N's coprimes in $\{1, \ldots, N-1\}, * \mod N$. Proof: GCD with N is 1, so use extended Euclid's alg to find inverses. If p prime; -1 := p-1; $\sqrt{1} \equiv \pm 1 \mod p$.

8.1. **Order.** N=pq; p, q primes: order = totient function: $|Z_N^*| = \varphi(N) = (p-1)(q-1)$: we discard multiples of p, q. Also, if $N = \prod p_i^{e_i}$, $\varphi(N) = \prod (p_i - 1) p_i^{e_i - 1}$.

(Euler's theorem). $a^{\varphi(N)} \equiv 1 \mod N$: Take $a, a^2 \ldots a^k = e$; this is a subgroup of Z_N^*; by Lagrange (see group theory in algebra ref), $k|\varphi(N)$.

$N = \prod p_i^{e_i}$. $\frac{|Z_N^*|}{|Z_N^+|} = \frac{\varphi(N)}{N} = \prod_{i=1}^t \frac{p_i - 1}{p_i} \geq \prod_{i=1}^t \frac{i}{i+1} = \frac{1}{1+t} \geq \frac{1}{1+\log_2 N}$.

So, **Fermat's little theorem**: p prime: $a^p \equiv a \mod p$.

8.2. **Primitive roots.** Aka generator. If $S = Z_n^*$, g is primitive root of n. Z_p^* for prime p always has primitive root [**Find proof**]. 7 has primitive roots 3, 5. $1, 2, 4, p^k, 2p^k$ have primitive roots for p odd prime and $k \geq 1$.
[**Find proof**][**Incomplete**]

The number of primitive roots, if there are any, is $\phi(\phi(n))$. (See group theory in algebra ref)

8.3. **Primitive root test.** g is primitive root of n iff its multiplicative order is $\phi(n)$: else it generates a subgroup. Efficiently see if g is a generator: find prime factors of $\phi(n) = \prod_i p_i$, keep seeing if $g^{\frac{\phi(n)}{p_i}} = 1$.

9. Quadratic residues

QR_n: set of squares mod n. Quadratic non residues. If $a \in QR_n, aRn$, else a N n.

Finding $\sqrt{x}$ same as solving $y^2 = x \mod n$, or factoring $(y^2 - x) \mod n$.

9.1. QR_p **for odd prime p.** As structure of Z_p^* cyclic; writable as $\left\{g^i\right\}$ for primitive root g; only even powers $\left\{g^{2i}\right\}$ are squares. So, $|QR_p| = |Z_p^*|/2$.

1 has exactly 2 roots: ± 1, and no more: $x^2 - 1 \mod p = (x-1) \mod p(x+1) \mod p = 0$ so x-1 = 0 mod p or x+1 = 0 mod p. $g^{\frac{p-1}{2}} = -1$. $\sqrt{g^{2i}} = \pm g^i$ by Euler thm.

9.1.1. *Jacobi symbol.* $(\frac{a}{p}) = 0$ if $p|a$; +1 if a R p, $p \nmid a$; -1 if a N p.

Legendre: generalization to n=pq; $(\frac{a}{n})$ = -1 if a N n; if a R n, $(\frac{a}{n}) = 1$, but can't tell if a R n given $(\frac{a}{n}) = 1$.

9.2. QR_n **for p, q odd primes; n = pq (Blum integer).** $\exists 4\ \sqrt{1}$: take $x^2 = 1 \mod n$; ± 1 are obvious roots; Chinese remainder thm solutions s for $x = 1 \mod p; x = -1 \mod q$ and t for $x = -1 \mod p; x = +1 \mod q$ are the other two. As square roots appear in pairs, s = -t. To find the non trivial square roots, must know p, q.

Similarly, for any odd $m = m_1 m_2$, 1 has ≥ 4 roots.

So, any $a^2 \in QR_n$ has ≥ 4 roots: $a\sqrt{1}$. So, $4^{-1}|Z_n^*| \leq |QR_n|$.