

Computational Number Theory 2

Zeph Grunschlag

Homomorphisms

DEF: A function $f : R_1 \rightarrow R_2$ between rings is called a **ring homomorphism** if for all x, y

- $f(x + y) = f(x) + f(y)$
- $f(x \cdot y) = f(x) \cdot f(y)$
- and $f(1) = 1$

Note: it follows that $f(0) = 0$, $f(-x) = -f(x)$, and for invertible elements $f(x^{-1}) = f(x)^{-1}$

Example: For M divisible by m $f : \mathbb{Z}_M \rightarrow \mathbb{Z}_m$ defined by $f(n) = n \bmod m$ is homomorphism.

2

Isomorphisms

DEF: A homomorphism that is bijective is called an **isomorphism**.

Example: Index theorem says that the exponential function $f : \mathbb{Z}_{p-1} \rightarrow \mathbb{Z}_p^*$ defined by $f(i) = x^i \bmod p$ is an isomorphism if x is primitive.

NOTE: \mathbb{Z}_p^* is viewed as a ring if re-interpret multiplication as addition, exponentiation by index as multiplication, 1 as 0, and x as 1.

3

Chinese Remainder Theorem

Suppose $M = m_1 \cdot m_2 \cdots m_r$. There is a homomorphism $f : \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$ defined by $f(n) = (n \bmod m_1, \dots, n \bmod m_r)$

NOTE: domain and codomain have same size

THM: If all the m_i are pairwise relatively prime, then f is an isomorphism. Furthermore, the inverse is given by a linear function

$$g(n_1, n_2, \dots, n_r) = (c_1 n_1 + c_2 n_2 + \dots + c_r n_r) \bmod M$$

$$\text{with } c_i = \left(\frac{M}{m_i}\right) \cdot \left[\left(\frac{M}{m_i}\right)^{-1} \bmod m_i\right]$$

4

Algebraic Implications

Assuming $N = n_1 \cdot n_2 \cdots n_r$ with all n_i pairwise relatively prime.

LEMMA1: There is an isomorphism on multiplicative groups $\mathbb{Z}_N^* \approx \mathbb{Z}_{n_1}^* \times \mathbb{Z}_{n_2}^* \times \cdots \times \mathbb{Z}_{n_r}^*$

COR: $\phi(N) = \phi(n_1) \cdot \phi(n_2) \cdots \phi(n_r)$

LEMMA2: A linear transformation on the space \mathbb{Z}_N^k (i.e. a k by k square matrix) is invertible iff it is invertible modulo each n_i .

COR: $M_k(N)^* \approx M_k(n_1)^* \times \cdots \times M_k(n_r)^*$

5

Square Roots mod- pq For Prime Factors p, q

LEMMA: Let $n = pq$ with p, q different odd primes. For each quadratic residue $s \pmod n$ there are exactly **four** square roots of s . Furthermore, if $\pm r_p, \pm r_q$ are the square roots of s respectively mod p and mod q , then the square roots of $s \pmod n$ are all the sums:
 $[\pm q(q^{-1} \pmod p)r_p + \pm p(p^{-1} \pmod q)r_q] \pmod n$

THM: Factoring n and taking square roots mod n are equivalent in the class BPP.

6

Taking e'th Roots and Factoring

Recall: for $a \in \mathbb{Z}_n^*, b = a^e \pmod n$ such that the exponent e is relatively prime to $\phi(n)$, "e'th root" of b calculated by:

$$a = b^{e^{-1} \pmod{\phi(n)}} \pmod n$$

RESULT: If factorization of n is known, taking e'th roots mod n is tractable.

FACT: For $n = pq$, knowing $\phi(n)$ gives p, q .

PARTIAL CONVERSE: If know e'th root exponent d then can factor n .

FULL CONVERSE? - Open problem

7

Miller-Rabin Primality

Let n be an odd number. Let q be the odd part of $n-1$, so $n-1 = 2^k q$, and b be any integer in \mathbb{Z}_n .

DEF: n is a **strong pseudoprime relative to b** if $b^q \equiv_n 1$, or $b^{2^i q} \equiv_n -1$ for some $i < k$.

THM: For any odd composite n and random b $\Pr(n \text{ is strong pseudoprime rel. } b) \leq 1/4$.

NOTE: Non-prime pseudoprimes much rarer in practice. Worst case probability for $n = 9$.

Miller-Rabin-Primality-Test(positive integer n)

if ($n=1$ OR n is even) return "NO"

choose $b \in [2, n-2]$ at random

if ($\gcd(b, n) > 1$) return "NO"

return TestIfStrongPseudoPrime(n, b)

8