Computational Number Theory 2

Zeph Grunschlag

Homomorphisms
DEF: A function \( f : R_1 \to R_2 \) between rings is called a \textbf{ring homomorphism} if for all \( x, y \)

\[
\begin{align*}
&f(x + y) = f(x) + f(y) \\
&f(xy) = f(x)f(y)
\end{align*}
\]

and \( f(1) = 1 \)

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

Example: For \( M \) divisible by \( m \) \( f : \mathbb{Z}_M \to \mathbb{Z}_m \)

defined by \( f(n) = n \mod m \) is homomorphism.

\[
f : R_1 \to R_2
\]

\[
f(x-1) = f(x) - 1
\]

\[
f : \mathbb{Z}_M \to \mathbb{Z}_m
\]

Isomorphisms
DEF: A homomorphism that is bijective is a \textbf{isomorphism}.

Example: Index theorem says that the exponential function defined by \( f(i) = x^i \mod p \) 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.

Chinese Remainder Theorem
Suppose \( M = m_1 \cdot m_2 \cdots m_r \). There is a homomorphism \( f : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r} \)

defined by \( f(n) = (n \mod m_1, \ldots, n \mod m_r) \)

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

\[
g(n_1, n_2, \ldots, n_r) = (c_1n_1 + c_2n_2 + \ldots + c_rn_r) \mod M
\]

with \( c_i = \left( \frac{M}{m_i} \right) \cdot \left( \frac{M}{m_i} \right)^{-1} \mod m_i \)
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**: \( M_k(N)^* \approx M_k(n_1)^* \times \cdots \times M_k(n_r)^* \)

Taking e’th Roots and Factoring

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

\[
a = b^{e^{-1} \mod \phi(n)} \mod n
\]

**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

Square Roots mod-pq

For Prime Factors p, q

**LEMMA**: Let \( n = pq \) with \( p, q \) different odd primes. For each quadratic residue \( s \mod n \) 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 \( s \mod n \) are all the sums:

\[
[\pm q(q^{-1} \mod p) r_p + \pm p(p^{-1} \mod q) r_q] \mod n
\]

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

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 \( b^q \equiv 1 \mod n \), or \( b^{2^i q} \equiv -1 \mod n \) for some \( i < k \).

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

**NOTE**: Non-prime pseudoprimes much rarer in practice. Worst case probability for \( n = 9 \).

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

1. if (\( n=2 \) OR \( n \) is even) return “NO”
2. choose \( b \in [2, n-2] \) at random
3. if ( \( \gcd(b,n) > 1 \) ) return “NO”
4. return TestIfStrongPseudoPrime(n,b)