CS203B, Assignment 5

Prof. Manindra Agarwal

September 2016

Rings and fields have found a number of applications in computer science. This includes desgining cryptosystems and related problems, algorithms for machine learning, image recognition, error-correcting codes etc. In this assignment, we take a look at one of them: *primality testing.* In this problem, a number n is given and one needs to decide if it is prime. It can be done simply by trying to divide n by all numbers $\leq \sqrt{n}$, however, for large values of n (imagine 100 digit long numbers), this method takes too much time. Several faster methods to solve this problem are known. We describe one of them. It is an example of how the rings and fields come to unexpected help in designing algorithms.

Given number n, define ring $R = Z_n[x]/(x^r - 1)$ for a carefully chosen number r (r is much smaller than n; of the order of square of the number of digits in n). Below, we require a number of properties of r. The number can be chosen to satisfy all of them.

1. Prove that R is a finite commutative ring with exactly n^r elements.

2. An element of R is a polynomial in x of degree $< r$ with coefficients from Z_n. We use the notation $a(x)$ to represent elements of R. Define map $\phi : R \mapsto R$ as: $\phi(a(x)) = a^n(x)$. It is obvious that
$$\phi(a(x) \cdot b(x)) = \phi(a(x)) \cdot \phi(b(x)).$$
Prove that ϕ is a ring homomorphism if and only if
$$\phi(a(x)) = a(x^n)$$
for every $a(x) \in R$.

3. Prove that when n is prime, ϕ is a ring homomorphism.

4. On the other hand, when n is a composite number, ϕ is not a ring homomorphism. Show this for the ring $Z_6[x](x^3 - 1)$.

Let p be a prime divisor of n, and $Q(x)$ an irreducible factor of $x^r - 1$ of degree $d > 1$ (the choice of r ensures that Q can be chosen to have large degree). Let $F = Z_p[x]/(Q(X))$. F is a finite field of size p^d. Define $\psi : R \mapsto F$ to be the map given by
$$\psi(a(x)) = a(x) \pmod{p, Q(x)}$$
where first the polynomial $a(x)$ is reduced modulo $Q(x)$ and then the coefficients of the remainder are reduced modulo p.

5. Prove that ψ is an onto ring homomorphism with kernel being the ideal $(p, Q(x)) = pR + Q(x)R$.

6. Prove that if $\phi(a(x)) = a(\phi(x))$ in R, then $\phi(\psi(a(x)) = \psi(a(x^n))$ in F.

For composite n: with appropriate r, it can be shown that the number of $b(x)$ of F for which $\phi(b(x)) = b(x^n)$ is less than $\binom{r+d}{d}$.

For prime n: the number of $b(x)$ of F for which $\phi(b(x)) = b(x^n)$ is exactly $|F| = p^d$. This number is larger than $\binom{r+d}{d}$ for an appropriate r.

This difference in the properties of ϕ is exploited to decide if n is prime. Consider elements $x + \ell$ for $1 \leq \ell \leq r$.

7. Prove that if $p \geq r$, these elements are distinct in F.

8. Let

$$S = \{\prod_{\ell=1}^{r} (x + \ell)^{m_\ell} \mid m_\ell \geq 0\}.$$

Set S is clearly a group under multiplication. Prove that the size of S is at least $\binom{r+d}{d}$.

Once we have all the above properties, the algorithm is quite simple:

> Choose an r satisfying all of above conditions. Verify that there are no prime divisors of n that are $\leq r$. For every ℓ, $1 \leq \ell \leq r$, verify that $\phi(x + \ell) = x^n + \ell$ in the ring R.

9. Prove that when n is composite, one of the above verifications will fail.