| | |
|---|---|
| **6.885 Algebra and Computation** | October 31, 2005 |

Lecture 14

*Lecturer: Madhu Sudan* — *Scribe: Sophie Rapoport*

Today, we give a brief review of factorization of polymnomials, then begin our study of primality testing by giving some simple but inefficient algorithms for testing the primality or compositeness of an integer, and then introducing a more sophisticated, recent method for testing primality based on the work of Agarwal et al.

# 1 Review of Factorization

We know how to factor over many rings:

- If $R$ is a UFD, we know roughly how to factor over $R$
- If $R$ is a UFD, we can factor over $R[x]$ using resultants, Hensel lifting, linear algebra, and lattice algorithms.
- We can also factor over $R[x]/h(x)$ where $h(x)$ is an irreducible polynomial, though this factorization is not always trivial.
- There exist basic rings over which we cannot factor (i.e. $\mathbb{Z}$), but to factor over more complex rings, we can describe each ring starting with smaller subrings and use a finite number of extensions to describe the entire ring.

# 2 Primality testing

## 2.1 History

The subject of primality testing can be considered as attempting to answer the following two questions:

1. What does a proof of the statement "$n$ is prime" look like?
2. What does a proof of the statement "$n$ is composite" look like?

Note that a "proof" consists of $k$ bits of information, where $k$ is polynomial in $\log(n)$, and a polynomial time algorithm to verify the claim that $n$ is prime or composite.

### 2.1.1 Proofs of Compositeness of $n$

An obvious proof of compositeness for a number $n$ would be a factorization $n = pq$, where $p, q \neq 1$. However, as stated above, we don't have an efficient method to factorize over $\mathbb{Z}$, so such a proof is difficult to find.

We use the observation $\mathbb{Z}_n \approx \mathbb{Z}_p \times \mathbb{Z}_q$ and the Chinese Remainder Theorem to gain information about $\mathbb{Z}_n$.

From the CRT, we have that if $\exists$ $a$,$k$ such that $a^{2k} \equiv 1 \pmod n$ and $a^k \not\equiv \pm 1 \pmod n$, or if $a^{n-1} \not\equiv 1 \pmod n$, then $n$ is composite. The Solovay-Strasson and Miller-Rabin algorithms exploit this property to determine if a given $n$ is composite. These algorithms pick $a$ at random, and with probability greater than $1/2$, there exists a $k$ satisfying this compositeness criterion.

However, if we find no such pairs $a$,$k$, we have not gained any information - this is not a guarantee that $n$ is prime.

### 2.1.2 Proofs of primality of $n$

Pratt gave an algorithm for proving $p$ prime using a prime factorization of $p-1$ (and other conditions), but it is VERY hard to find such a proof.

Goldwasser-Killian and Adelman-Huang (1986-88) gave randomized polynomial time proofs of primality as a strategy for finding primes between $n$ and $2n$, but these algorithms are beyond the scope of this class.

We use an alternate method to prove primality based on the following proof of compositeness:

## 2.2 Agarwal-Biswas Proof of Compositeness

Agarwal and Biswas developed this algorithm in 1999. Rather than using the Chinese Remainder Theorem, they used the following simple fact from number theory:

**Claim 1** $n|\binom{n}{i}\forall i$ *iff* $n$ *is prime.*

**Proof** $\binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i(i-1)\cdots 1}$ by definition.

If $n$ is prime, $(n, n-k) = 1$ and $(n, k) = 1\ \forall k$. Therefore, $(n, \frac{(n-1)\cdots(n-i+1)}{i(i-1)\cdots 1}) = 1$, hence $n|(n\frac{(n-1)\cdots(n-i+1)}{i(i-1)\cdots 1} = \binom{n}{i}$.

If $n$ is composite, $n = pq$, where $p$ is prime. Then we write $\binom{n}{p} = \frac{n}{p}\cdot\frac{(n-1)\cdots(n-p+1)}{(p-1)\cdots 1}$, observing that all the factors in the numerator and denominator of $\frac{(n-1)\cdots(n-p+1)}{(p-1)\cdots 1}$ are relatively prime to $p$, so that the whole fraction is relatively prime to $p$ (and relatively prime to $n$). We already know that $n \not| \frac{n}{p}$, so $n \not|\binom{n}{p} = \frac{n}{p}\cdot\frac{(n-1)\cdots(n-p+1)}{(p-1)\cdots 1}$. ■

Given this claim, we could construct a straightforward primality test for $n$ by verifying if $n|\binom{n}{i}$, but we don't have an efficient way to compute $\binom{n}{i}$.

Instead, we consider the binomial expansion of $(x+a)^n = x^n + \binom{n}{1}x^{n-1}a + \cdots + \binom{n}{n-1}xa^{n-1} + x^n$. Taken modulo $n$, this equality yields $(x+a)^n = x^n + a^n + \sum_{i=1}^{n-1}\binom{n}{i}x^i a^{n-i} \equiv x^n + a^n \pmod{n}$ iff $n$ is prime. We can further simplify this congruence to $(x+a)^n \equiv x^n + a \pmod{n}$.

From this fact, we derive the following algorithm:

Given $n$,

Pick $h(x)$ a monic polynomial of degree $poly(log(n))$

Then consider $(x+1)^n \equiv x^n + 1 \pmod{n), h(x}$.

We can use repeated squaring to reduce the equation $\pmod{h(x)}$ at each step. If this congruence holds for many polynomials $h_i(x)$, it holds for $LCM(h_i(x))$, and we can thereby extend the result.

If $n$ is composite, then $(x+1)^n \not\equiv x^n + 1$, so there exists $h(x)$ for which the above congruence does not hold. We therefore limit ourselves to the case where $h(x) = x^r - 1$.

## 2.3 Agarwal, Kayal, Saxena Proof of primality

This method for testing compositeness was extended by Agarwal, Kayal, and Saxena in 2002 to test for primality.

**Theorem 2** *If* $\forall r \in 1, \ldots, \log^3(n)$ *and* $\forall a \in 1, \ldots, \log^2(n)$,
$(x+a)^n \equiv x^n + a \pmod{n, x^r - 1}$ *and* $r \not| n$, *then* $n$ *is a prime power.*

From the knowledge that $n$ is a prime power, it is straightforward to determine if $n$ is in fact prime.

Recall that for primes $p$, $f(x)^p \equiv f(x^p) \pmod{p}$.

We make the following observation:

Suppose that we've run the test for compositeness and found only polynomials $f(x)$ satisfying $f(x)^n = f(x^n)$.

If $n$ is composite, $n = pq$, where $p$ is prime, so $f(x^n) \equiv f(x)^n \pmod{p, x^r - 1}$ AND $f(x^p) \equiv f(x)^p \pmod{p, x^r - 1}$. Say that $p|n$ but that $n \neq p^i\ \forall i$, and that $h(x)$ is an irreducible factor of $\frac{x^r-1}{x-1}$ in $\mathbb{F}_p[x]$. Then let us examine $K = \mathbb{F}_p[x]/h(x)$. Note that we can derive information about the function $h(x)$, but that it doesn't matter for our purposes what $h$ we pick.

**Definition 3** *Suppose that $R = \mathbb{Z}[x]/(h(x), q(x))$. We say that $f$ is introspective with respect to $m$ if $f(x)^m = f(x^m)$ in $R$.*

**Definition 4** *For integers p,n, and r, we define $t = t_{p,n,r} = |\{p^i n^j \pmod{r} | i, j \in \mathbb{Z}\}|$*

**Lemma 5 (Lemma 1)**
1. *If $f$ and $g$ are introspective with respect to $R$, then so is $f \cdot g$.*
2. *If $f$ is introspective with respect to $m_1$ and $m_2$ in $R = \mathbb{Z}_n[x]/(x^r - 1)$, then $f$ is introspective with respect to $m_1 \cdot m_2$ in $R$.*

**Proof**

1. $f$, $g$ are introspective, so $f(x)^m = f(x^m)$ and $g(x)^m = g(x^m)$ in $R$. Then, $(f \cdot g)(x^m) = f(x^m) \cdot g(x^m) = f(x)^m \cdot g(x)^m = (f(x) \cdot g(x))^m$.
2. We have $f(x)^{m_1} = f(x^{m_1})$ and $f(x)^{m_2} = f(x^{m_2})$. Now, $f(x)^{m_1 m_2} = (f(x)^{m_1})^{m_2}$. Let us write $x^{m_1} = z$, then $f(x)^{m_1 m_2} = f(z)^{m_2} = f_{R'}(\mathbb{Z}^{m_2}) \pmod{z^r - 1}$, where $R' = \mathbb{Z}/(x^r - 1)$. We then substitute back in for $z$, obtaining $f(x_1^m m_2) \pmod{x^{m_1 r} - 1}$. Here we use a polynomial so that $x^r - 1 | x^{m_1 r} - 1$. By this construction, we have the desired identity for any ring R, provided that the congruence is considered $\pmod{x^r - 1}$. We let $q(x) = x^r - 1$, so that $q(x) | q(x^{m_1})$.

■

Now that we have introduced this notion of introspection, our goal is to use this property to write out identities in a field.

**Lemma 6** *Suppose $p|n$, $n \neq p^i$, $h(x)$ is irreducible and monic in $\mathbb{F}_p[x]$. Then $\exists$ a polynomial $p$ in $\mathbb{F}_p[y]$ with coefficients $\pm 1$ of degree $\leq n^t$ so that $\forall f \in \mathbb{F}_p[x]$ such that $f$ is introspective with respect to $n$ in $K = \mathbb{F}_p[x]/h(x)$, $P(f) = 0$ in $K$.*

To prove this lemma, we begin with a weaker statement and the following claim:

**Claim 7** *If $f$ is introspective with respect to $m_1$ and $m_2$ in $R = \mathbb{Z}_n[x]/(x^r - 1)$ and $m_1 \equiv m_2 \pmod{r}$. Then $f(x)^{m_1}$=$f(x)^{m_2}$ in $R$.*

Note that this claim gives us an actual ring identity and also establishes $f$ as a root of the polynomial $P(Y) = y_1^m - y_2^m$.

**Proof**

We have that $f(x)^{m_1} = f(x^{m_1})$ and that $f(x)^{m_2} = f(x^{m_2})$. Furthermore, $f(x^{m_1 + ir}) \equiv f(x^{m_1}) \equiv f(x^{m_2}) \pmod{x^r - 1}$ since $x^r \equiv 1 \pmod{r}$ and $x^{m_1} \equiv x^{m_2 + ir}$. Our goal is to find such a pair $m_1$, $m_2$ so that $f$ is a root of the polynomial $P(y) = y^{m_1} - y^{m_2}$.

Suppose that $f$ is introspective with respect to $n$. Then $f$ is also introspective with respect to $n^2$, $n^{i+1}$,. . .,$n^r$, so there exists a pair $i$,$j$ so that $n^i \equiv n^j \pmod{r}$. Letting $m_1 = n^i$ and $m_2 = n^j$, we have a pair satisfying the conditions of our claim, and therefore, we have a polynomial $P$ of degree less than $n^r$.

We further show that $deg(P) < n^t$ (where t is $t_{p,n,r}$ as defined above). Compare $p^i n^j \pmod{r}$ to $n$,$n^2$,. . .,$n^r$. There are at most $t$ elements in this sequence by definition of $t$.

We can limit the degree of $p$ even further as follows. $n$ is prime, so we consider the ring $K = \mathbb{F}_p[x]/h(x)$ where $p$ prime. $p$ is prime, so $f$ is introspective with respect to $p$.

Now, consider the following integers:

$$\begin{array}{ccccc} 1 & n & n^2 & \dots & n^i \\ p & pn & pn^2 & \dots & pn^i \\ p^2 & p^2n & p^2n^2 & \dots & p^2n^i \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p^j & p^jn & p^jn^2 & \dots & p^jn^i \end{array}$$

Since $f$ is introspective with respect to $p$ and with respect to $n$, $f$ is introspective with respect to all the integers listed in the table, and all of these values are distinct integers. Set $i, j = \sqrt{t}$. Then all integers in the table are $\leq n^{2\sqrt{t}}$, and there are at least $t + 1$ elements in the array. Hence, by the pigeonhole principle, there exists a pair $l$,$k$ and a pair $l'$,$k'$ so that $p^k n^l \equiv p^{k'} n^{l'} \pmod{r}$. Then $deg(P) \leq n^{2\sqrt{t}}$.

■

# 3 Continuation

We note that we can construct infinitely many such polynomials, but that they are not all distinct modulo $h$. Next time, we show that if $n$,$p$,$h$, and $K$ are as before, the following statement holds:

**Lemma 8** *Let $f$,$g$ be polynomials in $\mathbb{Z}_p[x]$ of degree less than $t$, both introspective with respect to $n$ in $K$. Then* $f \not\equiv g \pmod{h(x)}$.