

CSE203 - Counting Techniques in Designing Probabilistic Algorithms

Lecturer: Russell Impagliazzo
Scribes: Sarah Shoup and Scott Yilek

Tuesday, May 2, 2006

Today: Algebraic counting arguments and primality testing as an example.

Fermat's Little Theorem. *If p is prime, then*

$$\forall 1 \leq x \leq p-1, x^{p-1} \equiv 1 \pmod{p}$$

We will prove this theorem a bit later. For now, let's look at a probabilistic algorithm to test for primality:

1 Peralta's Primality Testing

Algorithm IsPrime(N)

if $N = M^k, M, k > 1$ **output** "Not Prime" // Rules out perfect squares

repeat t times: // t is small and is the 'tradeoff' value

 Pick $x_i \in_U \{1, \dots, N-1\}$

$z_i \leftarrow x_i^{(N-1)/2} \pmod{N}$ //using repeated squaring method

if $\exists$ such that $z_i \notin \{1, -1\}$, **output** "Not Prime"

if all $z_i = 1$ or all $z_i = -1$, **output** "Probably not prime" // primes should have even distribution

else output "Probably prime"

1.1 Correctness

We would like to be able to say something about the correctness of this algorithm. More specifically, we wish to show that if the algorithm outputs "Not prime", then N is not a prime; if it outputs "probably not prime" or "probably prime", we wish to show that with high probability N is composite or prime, respectively. The analysis of the algorithm first requires some knowledge of definitions and theorems from group theory.

1.1.1 Groups

A *group* is defined as a set of objects, an operation on those objects, an identity object, and an inverse. More formally, a *group* $\mathbf{G}$ consists of

Set of objects	: $\mathbf{G}$
Operation	: $\cdot : \mathbf{G} \times \mathbf{G} \rightarrow \mathbf{G}$
Identity	: $1 \in \mathbf{G}$
Inverse	: $^{-1} : \mathbf{G} \rightarrow \mathbf{G}$

The group also has three properties:

Associative	: $(g \cdot h) \cdot i = g \cdot (h \cdot i)$
Identity	: $g \cdot 1 = 1 \cdot g = g$
Cancellation	: $g \cdot g^{-1} = 1 = g^{-1} \cdot g$

Abelian groups also have one other property

$$\text{Commutative} \quad : \quad a \cdot b = b \cdot a$$

What are some standard groups (or groups we might find useful)? The first is an Abelian group, the integers with addition mod N , denoted ${}^+N$:

$$\begin{aligned} {}^+N & : \{0, \dots, N-1\} \\ \text{Identity} & : 0 \\ \text{Operation} & : g \cdot h \stackrel{\text{def}}{=} (g+h) \mod N \\ \text{Inverse} & : g^{-1} \stackrel{\text{def}}{=} -g = N-g \end{aligned}$$

Another useful group is $\mathbb{Z}_N^*$:

$$\begin{aligned} \mathbb{Z}_N^* & : \{x | 1 \leq x \leq N-1 \wedge \gcd(x, N) = 1\} \\ \text{Identity} & : 1 \\ \text{Operation} & : g \cdot h \stackrel{\text{def}}{=} (g \cdot h) \mod N \end{aligned}$$

What about the inverse? Does one even exist? For some x look at $\{1, x, x^2, x^3, \dots\}$. Taken mod N , eventually elements must start repeating. Thus,

$$\exists_{i < j} \text{ s.t. } x^i \equiv x^j \mod N$$

so $N | x^i - x^j$ and thus $N | x^i(x^{j-i} - 1)$. Since N cannot divide x^i (since x and N are relatively prime), only the right side “helps” with the divisibility. So,

$$\exists_k, N | x^k - 1 \Rightarrow x^k \equiv 1 \mod N \Rightarrow x(x^{k-1}) \equiv 1 \mod N \Rightarrow x^{-1} \equiv x^{k-1}$$

So we know inverses exist for all elements in the set. The other group properties are straight forward to show, so we can conclude that $\mathbb{Z}_N^*$ is in fact a group.

1.1.2 Subgroups

Our next important algebraic construct is the *subgroup*. A *subgroup* of $\mathbf{G}$ is a set $\mathbf{H} \subseteq \mathbf{G}$, so that

$$\begin{aligned} 1 & \in \mathbf{H} \\ h \in \mathbf{H} & \Rightarrow h^{-1} \in \mathbf{H} \\ h_1, h_2 \in \mathbf{H} & \Rightarrow h_1 \cdot h_2 \in \mathbf{H} \end{aligned}$$

In other words, a H is subgroup of G if it is a subset of G and it is itself a group under G 's group operation. One of the two important things we will use to prove the correctness of the given primality testing algorithm is the following theorem.

Theorem 1. *If $\mathbf{G}$ is a finite group, and $\mathbf{H}$ is a subgroup of $\mathbf{G}$, then*

$$|\mathbf{H}| \mid |\mathbf{G}|$$

Proof. The idea we will use is to show that $\mathbf{G}$ can be partitioned into blocks which are all the size of $\mathbf{H}$. To do this we will first define an equivalence relation $\sim_{\mathbf{H}}$.

$$g_1 \sim_{\mathbf{H}} g_2 \stackrel{\text{def}}{=} g_1 \cdot g_2^{-1} \in \mathbf{H}$$

Recall that for a relation to be an equivalence relation it must be transitive, symmetric, and reflexive.

Transitive: If $g_1 \sim_{\mathbf{H}} g_2$ and $g_2 \sim_{\mathbf{H}} g_3$, then $g_1 \cdot g_2^{-1} \in \mathbf{H}$ and $g_2 \cdot g_3^{-1} \in \mathbf{H}$. Multiplying these, we get $g_1 \cdot g_2^{-1} \cdot g_2 \cdot g_3^{-1} = g_1 \cdot g_3^{-1} \in \mathbf{H}$ and so $g_1 \sim_{\mathbf{H}} g_3$.

Symmetric: If $g_1 \sim_{\mathbf{H}} g_2$ then $g_1 \cdot g_2^{-1} \in \mathbf{H}$, but then so is the inverse $(g_1 \cdot g_2^{-1})^{-1} \in \mathbf{H}$. This inverse equals $g_2 \cdot g_1^{-1}$ so $g_2 \sim_{\mathbf{H}} g_1$.

Reflexive: If $g \sim_{\mathbf{H}} g$, then $g \cdot g^{-1} \in \mathbf{H}$ which is true since the identity element is in $\mathbf{H}$.

Now that we have an equivalence relation, we can partition $\mathbf{H}$ into equivalence classes. We will define the set of things equivalent to an element g to be

$$\text{co-set}_{\mathbf{H}}(g) = \{hg | h \in \mathbf{H}\}$$

This is also called the left co-set since we are multiplying elements of H on the left side of g .

Claim 1.

$$|\text{co-set}_{\mathbf{H}}(g)| = |\mathbf{H}|$$

Proof. We want to show that the mapping $f(h) = hg$ is one-to-one. The range of f is the co-set, by definition. If we assume f is not one-to-one, then there exist distinct h_1, h_2 such that $h_1 \cdot g = h_2 \cdot g$. Then

$$\begin{aligned} (h_1 \cdot g) \cdot g^{-1} &= (h_2 \cdot g) \cdot g^{-1} \\ h_1 &= h_2 \end{aligned}$$

which contradicts that h_1, h_2 are distinct. So, the map must be one-to-one. The claim follows. $\square$

Getting back to the proof of the theorem, consider what happens if $\text{co-set}(g_1) \cap \text{co-set}(g_2) \neq \emptyset$. Then, there exists a g_3 such that $g_1 \sim_{\mathbf{H}} g_3$ and $g_2 \sim_{\mathbf{H}} g_3$. Then $g_1 \sim_{\mathbf{H}} g_2$ since $\sim_{\mathbf{H}}$ is an equivalence relation, and thus g_1 and g_2 belong to the same equivalence class. That is, $\text{co-set}(g_1) = \text{co-set}(g_2)$.

If we pick a maximal set $g_0 = 1, g_1, \dots, g_{t-1}$ that are not equivalent, then

$$\mathbf{G} = \bigcup_{i=0}^{t-1} \text{co-set}(g_i).$$

and $\text{co-set}(g_i) \cap \text{co-set}(g_j) = \emptyset, \forall i \neq j$. Therefore, $|\mathbf{G}| = |\mathbf{H}| \cdot t$ and thus $|\mathbf{H}| \mid |\mathbf{G}|$. $\square$

1.1.3 Proof of Fermat's Little Theorem

Let

$$\begin{aligned} p &\text{ be a prime} \\ x &\in \{1, \dots, p-1\} \\ \mathbf{H} &= \{1, x, x^2, x^3, \dots, x^i, \dots\} = \{1, x, \dots, x^{h-1}\} \end{aligned}$$

Here h is the smallest integer such that $x^h=1$, and thus $h = |\mathbf{H}|$. Then $x^{-1} = x^{h-1}$ since $x \cdot x^{h-1} = 1$, and thus inverses are closed within $\mathbf{H}$. Similarly, for any $x^i, x^j \in \mathbf{H}$, $x^i \cdot x^j = x^{i+j}$ is also in $\mathbf{H}$ (since $\mathbf{H}$ contains all powers of x). It follows that $\mathbf{H}$ is a subgroup of $\mathbb{Z}_p^*$. We call this the subgroup generated by x .

Because of the theorem from the previous section, $|\mathbf{H}| \mid |\mathbb{Z}_p^*|$ which means that $h \mid (p-1)$ since the size of $\mathbf{H}$ is h and the size of $\mathbb{Z}_p^*$ is $p-1$. It follows that $(p-1) = h \cdot t$ for some t . If we take some x and raise it to the $(p-1)$ th power, then:

$$(x^{p-1}) \equiv (x^{ht}) \equiv (x^h)^t \equiv 1^t \equiv 1 \pmod{p}$$

which ends the proof of Fermat's Little Theorem.

1.1.4 A general method for probabilistic algorithms

We can generalize our approach to finding a witness with property $\mathcal{P}$. We then concentrate on showing three properties:

1. All possible witnesses form a group $\mathbf{G}$.
2. All witnesses with $\neg\mathcal{P}$ form a sub-group $\mathbf{H}$.
3. $\mathbf{H} \subsetneq \mathbf{G}$ (in this case, we call $\mathbf{H}$ a proper subgroup of $\mathbf{G}$)

Since $|\mathbf{H}|$ divides $|\mathbf{G}|$ and property 3 ensures that $|\mathbf{H}| < |\mathbf{G}|$, we can conclude that $|\mathbf{H}| \leq \frac{1}{2}|\mathbf{G}|$. This means that if we pick a random witness, it has probability at least $1/2$ of having property $\mathcal{P}$.

In our primality testing algorithm, the witnesses for “not prime” (the first test under the loop) will be $x \in \mathbb{Z}_N^*$ with the property $\mathcal{P}$ that $x^{(N-1)/2} \notin \{1, -1\}$. Then, our subgroup of witnesses with property $\neg\mathcal{P}$ will be $\mathbf{H} = \{x \in \mathbb{Z}_N^* | x^{(N-1)/2} \bmod N \in \{1, -1\}\}$. Then, in the algorithm $\mathbf{H}$ will either be the entire group $\mathbb{Z}_N^*$ or with probability at least $1/2$, $x^{(N-1)/2} \notin \{1, -1\}$.

To prove the correctness, however, we still need the second major idea, which is presented next.

1.1.5 Fields and polynomials over fields

A *field* $\mathbf{F}$ is defined to be

- $\mathbf{F}$: A set of elements
- $+$: an abelian group operation on $\mathbf{F}$ with identity 0, inverse $-x$
- $\cdot$: an abelian group operation on $\mathbf{F} - \{0\}$ with identity 1, inverse $^{-1}$.

With the additional property

$$\text{Distributive} \quad : \quad x \cdot (a + b) = x \cdot a + x \cdot b$$

A *polynomial over $\mathbf{F}$ of degree d* is

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_dx^d$$

where $a_0, a_1, \dots, a_d \in F$. z is a root of f if $f(z) = 0$.

We will need the following theorem about polynomials:

Theorem 2. *If f is a polynomial of degree d over a field F and $f \neq 0$, then f has less than or equal to d roots (in F).*

We do not provide a proof of this theorem (but see last year’s notes), but will use it in our analysis. The canonical field for us will be the field in which p is a prime and $+, \cdot \bmod p$ are the field operations, so in particular, any degree d polynomial over the integers mod p has at most d roots mod p .

We now concentrate on the case where $\mathbf{H} = \mathbb{Z}_N^*$, which means that $x^{(p-1)/2} \in \{1, -1\}$ for all $x \in [1, \dots, p-1]$.

We claim that

$$\begin{aligned} \Pr_{x \in [1, \dots, p-1]} [x^{(p-1)/2} = 1] &= \Pr [x^{(p-1)/2} = -1] \\ &= \frac{1}{2} \end{aligned}$$

We know that for all $x \in [1, \dots, p-1]$ that one or the other is true (though we have not bothered to prove this). Because $x^{(p-1)/2} = a$ is a polynomial of degree $(p-1)/2$, we know that each equation must have less than or equal to $(p-1)/2$ roots (for $a = -1, 1$). But since these are the only two choices, both inequalities are tight and our probability is $1/2$.

1.1.6 Bringing it all together

Returning to proving the correctness of Peralta's algorithm, we make the following claim:

Claim 2. *If p is a prime greater than 2,*

$$\Pr[\text{Peralta's Algorithm does not output "Probably prime"}] \leq \frac{1}{2^{t-1}}$$

Proof. We know that since p is a prime, $x^{(p-1)/2}$ will be evenly distributed between 1 and -1. Peralta's algorithm will only fail to output "Probably prime" if on its t independent trials it finds the same value (1 or -1). We know that the following is true:

$$\begin{aligned} \Pr[\text{all 1s}] &= 1/2^t \\ \Pr[\text{all -1s}] &= 1/2^t \end{aligned}$$

Since either case will make our algorithm fail, we sum the probabilities and get $2/2^t = 1/2^{t-1}$. $\square$

Continuing proving the correctness of Peralta's algorithm,

Claim 3. *If N is a composite and $\mathbf{H} \neq \mathbb{Z}_N^*$*

$$\Pr[\text{algorithm outputs "Probably prime"}] \leq \frac{1}{2^t}$$

Proof. Recall that if $\mathbf{H} \neq \mathbb{Z}_N^*$ then $x^{(N-1)/2} \notin \{1, -1\}$ with probability at least $1/2$. So, if we execute t independent trials we will only have a $1/2^t$ chance of getting no values other than 1 or -1.

The remaining case is $\mathbf{H} = \mathbb{Z}_N^*$ and N is composite. We claim in this case, that either $x^{(p-1)/2} = 1$ for all $x \in \mathbb{Z}_N^*$ or $x^{(p-1)/2} = -1$ for all $x \in \mathbb{Z}_N^*$. Otherwise, let q_1, q_2 be distinct primes that divide N . Since all $(p-1)/2$ powers are either 1 or -1, but not all are 1, and not all are -1, there are x_1 and x_{-1} such that $x_1^{(N-2)/2} \equiv 1 \pmod{N}$ and $x_{-1}^{(N-2)/2} \equiv -1 \pmod{N}$. Now consider the element $x = x_1 \cdot (q_1^{-1} \pmod{q_2}) \cdot q_1 + x_{-1} \cdot (q_2^{-1} \pmod{q_1}) \cdot q_2$. Then:

$$\begin{aligned} x \pmod{q_2} = x_1 &\Rightarrow x^{(N-1)/2} \pmod{q_2} = 1 \\ x \pmod{q_1} = x_{-1} &\Rightarrow x^{(N-1)/2} \pmod{q_1} = -1 \end{aligned}$$

But given this, it cannot be that $x^{(N-1)/2} \pmod{N}$ is either 1 or -1, or we would have a contradiction. Then there is some element $x \in \mathbb{Z}_N^*$ but $x \notin \mathbf{H}$. It follows that $\mathbf{H} \neq \mathbb{Z}_N^*$, contrary to assumption.

So in this final case, the algorithm will only see all 1's or all -1's in the powers (or something that is neither, if an x not relatively prime to N is chosen) and will thus output "probably composite". $\square$