PRIMES is in coRP

Evan Chen

February 22, 2016

1 Preliminaries

1.1 Modular arithmetic

In middle school you might have encountered questions such as

Exercise 1. What is $3^{2016} \pmod{10}$?

You could answer such questions by listing out 3^n for small n and then finding a pattern, in this case of period 4. However, for large moduli this "brute-force" approach can be time-consuming.

Fortunately, it turns out that one can predict the period in advance.

Theorem 2 (Euler's little theorem)

(a) Let $\gcd(a,n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

(b) (Fermat) If p is a prime, then $a^p \equiv a \pmod{p}$ for every a.

Proof. Part (a) is a special case of Lagrange's Theorem (see [3, Chapter 1]): if G is a finite group and $g \in G$, then $g^{|G|}$ is the identity element. Now select $G = (\mathbb{Z}/n\mathbb{Z})^\times$. Part (b) is the case $n = p$. □

Thus, in the middle school problem we know in advance that $3^4 \equiv 1 \pmod{10}$ because $\phi(10) = 4$. This bound is sharp for primes:

Theorem 3 (Primitive roots)

For every p prime there's a $g \pmod{p}$ such that $g^{p-1} \equiv 1 \pmod{p}$ but $g^k \not\equiv 1 \pmod{p}$ for any $k < p-1$. (Hence $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)$.)

For a proof, see the last exercise of [4].

we will define the following anyways:

Definition 4. We say an integer n (thought of as an exponent) **annihilates** the prime p if

- $a^n \equiv 1 \pmod{p}$ for every prime p,
- or equivalently, $p - 1 \mid n$.

Theorem 5 (All/nothing)

Suppose an exponent n does not annihilate the prime p. Then more than $\frac{1}{2}p$ of $x \pmod{p}$ satisfy $x^n \not\equiv 1 \pmod{p}$.

Proof. Much stronger result is true: in $x^n \equiv 1 \pmod{p}$ then $x^{\gcd(n,p-1)} \equiv 1 \pmod{p}$. □

1.2 Repeated Exponentiation

Even without the previous facts, one can still do:

Theorem 6 (Repeated exponentation)
Given x and n, one can compute $x^n \pmod N$ with $O(\log n)$ multiplications mod N.

The idea is that to compute $x^{600} \pmod N$, one just multiplies $x^{512+64+16+8}$. All the x^{2^k} can be computed in k steps, and $k \le \log_2 n$.

1.3 Chinese remainder theorem

In the middle school problem, we might have noticed that to compute $3^{2016} \pmod 1)0$, it suffices to compute it modulo 5, because we already know it is odd. More generally, to understand $\pmod n$ it suffices to understand n modulo each of its prime powers.

The formal statement, which we include for completeness, is:

Theorem 7 (Chinese remainder theorem)
Let $p_1, p_2, \dots, p_m$ be distinct primes, and $e_i \ge 1$ integers. Then there is a ring isomorphism given by the natural projection

$$\mathbb{Z}/n \to \prod_{i=1}^{m} \mathbb{Z}/p_i^{e_i}.$$

In particular, a random choice of $x \pmod n$ amounts to a random choice of x mod each prime power.

For an example, in the following table (from [5]) we see the natural bijection between $x \pmod{15}$ and $(x \pmod 3, x \pmod 5)$.

$x \pmod{15}$	$x \pmod 3$	$x \pmod 5$	$x \pmod{15}$	$x \pmod 3$	$x \pmod 5$
0	0	0	8	2	3
1	1	1	9	0	4
2	2	2	10	1	0
3	0	3	11	2	1
4	1	4	12	0	2
5	2	0	13	1	3
6	0	1	14	2	4
7	1	2			

2 The RSA algorithm

This simple number theory is enough to develop the so-called RSA algorithm. Suppose Alice wants to send Bob a message M over an insecure channel. They can do so as follows.

- Bob selects integers d, e and N (with N huge) such that N is a semiprime and

$$de \equiv 1 \pmod{\phi(N)}.$$

- Bob publishes both the number N and e (the **public key**) but keeps the number d secret (the **private key**).

- Alice sends the number $X = M^e \pmod N$ across the channel.
- Bob computes
$$X^d \equiv M^{de} \equiv M^1 \equiv M \pmod N$$
and hence obtains the message M.

In practice, the N in RSA is at least 2000 bits long.

The trick is that an adversary cannot compute d from e and N without knowing the prime factorization of N. So the security relies heavily on the difficulty of factoring.

Remark 8. It turns out that we basically don't know how to factor large numbers N: the best known classical algorithms can factor an n-bit number in

$$O\left(\exp\left(\frac{64}{9}n\log(n)^2\right)^{1/3}\right)$$

time ("general number field sieve"). On the other hand, with a *quantum* computer one can do this in $O\left(n^2\log n\log\log n\right)$ time.

3 Primality Testing

Main question: if we can't factor a number n quickly, can we at least check it's prime?

In what follows, *we assume for simplicity that n is* ***squarefree***, i.e. $n = p_1p_2\dots p_k$ for distinct primes p_k, This doesn't substantially change anything, but it makes my life much easier.

3.1 Co-RP

Here is the goal: we need to show there is a random algorithm A which does the following.

- If n is composite then
  - More than half the time A says "definitely composite".
  - Occasionally, A says "possibly prime".
- If n is prime, A always says "possibly prime".

If there is a polynomial time algorithm A that does this, we say that PRIMES is in Co-RP. Clearly, this is a very good thing to be true!

3.2 Fermat

One idea is to try to use the converse of Fermat's little theorem: given an integer n, pick a random number $x \pmod n$ and see if $x^{n-1} \equiv 1 \pmod n$. (We compute using repeated exponentiation.) If not, then we know for sure n is not prime, and we call x a **Fermat witness** modulo n.

How good is this test? For most composite n, pretty good:

Proposition 9

Let n be composite. Assume that there is a prime $p \mid n$ such that $n-1$ does not annihilate p. Then over half the numbers mod n are Fermat witnesses.

Proof. Apply the Chinese theorem then the "all-or-nothing" theorem. □

Unfortunately, if n doesn't satisfy the hypothesis, then *all* the $\gcd(x,n)=1$ satisfy $x^{n-1} \equiv 1 \pmod n$!

Are there such n which aren't prime? Such numbers are called **Carmichael numbers**, but unfortunately they exist, the first one is $561 = 3 \cdot 11 \cdot 17$.

Remark 10. For $X \gg 1$, there are more than $X^{1/3}$ Carmichael numbers.

Thus these numbers are very rare, but they foil the Fermat test.

Exercise 11. Show that a Carmichael number is not a semiprime.

3.3 Rabin-Miller

Fortunately, we can adapt the Fermat test to cover Carmichael numbers too. It comes from the observation that if n is prime, then $a^2 \equiv 1 \pmod n \implies a \equiv \pm 1 \pmod n$.

So let $n-1 = 2^s t$, where t is odd. For example, if $n = 561$ then $560 = 2^4 \cdot 35$. Then we compute x^t, x^{2t}, $\dots$, x^{n-1}. For example [2] investigates the case $n = 561$ and $x = 245$:

	mod 561	mod 3	mod 11	mod 17
x	245	-1	3	7
x^{35}	122	-1	**1**	3
x^{70}	298	**1**	1	9
x^{140}	166	1	1	-4
x^{280}	67	1	1	-1
x^{560}	1	1	1	**1**

And there we have our example! We have $67^2 \equiv 1 \pmod{561}$, so 561 isn't prime.

So the Rabin-Miller test works as follows:

- Given n, select a random x and compute powers of x as in the table.
- If $x^{n-1} \not\equiv 1$, stop, n is composite (Fermat test).
- If $x^{n-1} \equiv 1$, see if the entry just before the first 1 is -1. If it isn't then we say x is a **RM-witness** and n is composite.
- Otherwise, n is "possibly prime".

How likely is probably?

Theorem 12

If n is Carmichael, then over half the $x \pmod n$ are RM witnesses.

Proof. We sample $x \pmod n$ randomly again by looking modulo each prime (Chinese theorem). By the theorem on primitive roots, show that the probability the first -1 appears in any given row is $\le \frac{1}{2}$. This implies the conclusion. □

Exercise 13. Improve the $\frac{1}{2}$ in the problem to $\frac{3}{4}$ by using the fact that Carmichael numbers aren't semiprime.

3.4 AKS

In August 6, 2002, it was in fact shown that PRIMES is in P, using the deterministic AKS algorithm [1]. However, in practice everyone still uses Miller-Rabin since the implied constants for AKS runtime are large.

References

[1] Agrawal, Manindra; Kayal, Neeraj; Saxena, Nitin (2004). "PRIMES is in P". *Annals of Mathematics* **160** (2): 781-793.

[2] Bobby Kleinberg, *The Miller-Rabin Randomized Primality Test* `http://www.cs.cornell.edu/courses/cs4820/2010sp/handouts/MillerRabin.pdf`

[3] Evan Chen, *An Infinitely Large Napkin*. `http://www.mit.edu/~evanchen/napkin.html`

[4] Evan Chen, *Orders Module A Prime*. `http://www.mit.edu/~evanchen/handouts/ORPR/ORPR.pdf`

[5] Horner Math Club MathCounts Materials: Problem Set 5.