CRYPTOGRAPHY HANDOUT 16

PRIMALITY TESTING

1. First Explorations

Recall that a **prime number** p is one in which the only factors are 1 and p.

Example. $p = 7, 31, 73, 311$ are prime numbers.

Question 1. *Consider the following numbers:* $292, 293, 299, 313, 427, 757, 759, 290829273$.
Determine if they are prime or not.
Discuss your strategies and any problems that arise with your group.

2. Factoring is not the same as Primality Testing

The following theorem is called the "basic principle" in your text (6.3 p. 176).

Theorem 1. *Let n be an integer and suppose there exist integers x and y with*

$$x^2 \equiv y^2 \bmod n,$$

but $x \not\equiv \pm y \bmod n$. Then n is composite. Moreover, $\gcd(x-y, n)$ gives a nontrivial factor of n.

Example. Let $x = 12$, $y = 2$ and $n = 35$ in the theorem. Work through the example and convince yourself the theorem works. Be sure to find a nontrivial factor of n too.

The next part will walk through the proof of the "basic principle." Work as a group to understand every line of the proof. First, let's prove a lemma:

Lemma 2. *Given integers a, b and c. Suppose $a \mid bc$ and $\gcd(a, b) = 1$. Then $a \mid c$.*

[**Prove this lemma before you move on.**]

Now we'll prove the theorem.

Proof. Let $d = \gcd(x - y, n)$.

Case one: If $d = n$, then $x \equiv y \bmod n$. [**Convince yourself this is true before you move on.**]

This is assumed not to happen, so $d \neq n$.

Case two: Suppose $d = 1$. Using the lemma, we can show that since n divides $x^2 - y^2 = (x - y)(x + y)$, then we must have that n divides $x + y$. [**Convince yourself this is true before you move on.**]

This is a contradiction since we assumed $x \not\equiv -y \bmod n$. Therefore, $d \neq 1$ and $d \neq n$, so d is a nontrivial factor of n.

□

Note. It turns out that showing a number is composite is an easier problem than it is to factor it, so the two problems are not the same.

Example. Recall Fermat's Little Theorem. It shows that if p is prime, then $2^{p-1} \equiv 1 \bmod p$ [**Why is this true?**]. We can use this to show that 35 is not prime without finding a factor by using *successive squaring*:

$$2^4 \equiv 16$$
$$2^8 \equiv 256 \equiv 11$$
$$2^{16} \equiv 121 \equiv 16$$
$$2^{32} \equiv 256 \equiv 11$$

Thus, we know that $2^{34} \equiv 2^{32}2^2 \equiv 11 \cdot 4 \equiv 8 \not\equiv 1 \mod 35$. Using the above result from Fermat's Little Theorem, we see that 35 cannot be prime, so it must be composite.

3. Primality Tests (which should be called Compositeness Tests)

The following tests give us different ways to test if a number is prime or not.

3.1. **Fermat Primality Test.** Let $n > 1$ be an integer. Choose a random integer a with $1 < a < n-1$. If $a^{n-1} \not\equiv 1 \bmod n$, then n is composite. If $a^{n-1} \equiv 1 \bmod n$, then n is probably prime.

Use the Fermat Primality Test on the following small examples to verify that they probably are prime or are composite.

1. $n = 292$

2. $n = 299$

3. $n = 757$

Some short SageMath code to do this would be:

```
n = 757
a = 3
a^(n-1)%n
```

3.2. **Solovay-Strassen Primality Test.** Let n be an odd integer. Choose several random integers a with $1 < a < n - 1$. If the Jacobi symbol is such that

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n$$

for some a, then n is composite. If

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n$$

for all a, then n is probably prime.

Use the Solovay-Strassen Primality Test on the following small examples to verify that they probably are prime or are composite.

1. $n = 293$

2. $n = 313$

3. $n = 427$

You might find that the results aren't as clear here. This is because you really need several random integers a here (and that isn't a good exercise to do by hand).

3.3. **SageMath.** SageMath has a built-in primality tester. The syntax is:

```
2 in Primes()
```

and the output will either be True or False (in the example, True, since 2 is prime).

Go back to your First Explorations examples and determine which one is prime using SageMath:

1. 292
2. 293
3. 299
4. 313
5. 427
6. 757
7. 759
8. 290829273