Lesson Sixteen

Math 6080 (for the Masters Teaching Program), Summer 2020

16. Fermat's Little Theorem. Let m be a natural number. Then:

Euler's Theorem. If $r \in \{1, ..., m-1\}$ is relatively prime to m, then

$$(r^{\phi(m)})\%m = 1$$

Examples. (a) $\phi(8) = 8 - 4 = 4$ and

$$1^4 = 1,\ 3^4 = 81, 5^4 = 625, 7^4 = 2401$$

verifies Euler's Theorem (they all have remainder 1 when divided by 8).

(b) $\phi(5)$ is also 4, and in that case:

$$1^4 = 1,\ 2^4 = 16,\ 3^4 = 81, 4^4 = 256$$

verify Euler's Theorem.

Proof. List all the numbers $r_1, ..., r_{\phi(m)} \in \{1, ..., m-1\}$ that are relatively prime to m. Multiply each of them by r. Since $rx = r_i$ has a unique solution for all i in modulo m arithmetic, it follows that:

$$r \cdot r_1,\ r \cdot r_2, ...,\ r \cdot r_{\phi(m)}$$

are just the same numbers $r_1, r_2, ..., r_{\phi(m)}$ in a different order. Thus:

$$r_1 \cdot r_2 \cdots r_{\phi(m)} = rr_1 \cdot rr_2 \cdots rr_{\phi(m)}$$

in modulo m arithmetic, *and we can divide both sides by each* r_i, leaving

$$1 = (r^{\phi(m)})\%m \quad \square$$

Corollary. If p is **prime** number and $r \in \{1, ..., p-1\}$, then:

$$(r^{p-1})\%p = 1$$

This Corollary is **Fermat's Little Theorem.**

Note. This gives a definitive criterion for showing that a number n is **not** prime without finding a factor of n. Namely, if you find that:

$$(r^{n-1})\%n \neq 1$$

for **any** $r \in \{2, ..., n_1\}$, then n is not a prime number.

At first glance, this doesn't seem to be a very checkable criterion when n is large. But in fact, it is quite the opposite!

Strategy for computing:

$$(r^m)\%n$$

when m and n are large numbers.

Step 1. Convert m to binary.

Step 2. By taking repeated squares, compute:

$$r, r^2, r^4 = (r^2)(r^2), r^8 = (r^4)(r^4), ... \text{ modulo } n$$

Step 3. Multiply together the powers of r (modulo n) corresponding to the 1's in the binary expansion of m to compute the mth power.

Example. Compute 2^{26} modulo 27.

Step 1. The binary expansion of 26 is 11010

Step 2. The successive squares of 2 modulo 27 are:

$$2, 2^2 = 4, 2^4 = 16, 2^8 = 256\%27 = 13, 2^{16} = 13^2 = 169\%27 = 7$$

Step 3. The answer is $2^{16} * 2^8 * 2^2 = 7 * 13 * 4 = 364\%27 = 13$.

Thus we conclude (without factoring it) that 27 is not a prime.

Exercise. Write Python code to prompt the user for a number m, ask the user for an additional number $r > 1$, and then follow the steps above to return the value of r^{m-1} modulo m, telling the user either:

- Our computation shows that m is not prime.

or

- Our computation does not determine if m is prime or not. Try another r.

Extended Project. When do the powers of 2 unmask a composite number?

Put the odd numbers m from 1 to 1000 into a table and test:

$$2^{m-1} \text{ modulo } m$$

Compare the odd numbers m for which $(2^{m-1})\%m = 1$ with the primes numbers. Which composite numbers snuck through?

A number m for which:

$$2^{m-1}, 3^{m-1}, 5^{m-1} \text{ and } 7^{m-1} \text{ are all 1 modulo } m$$

will be called a "good enough for government work" prime. Use Python to find the first "good enough for government work" prime number that is not prime.

Hint: It is very big. If we toss in 11 and 13, it is very, very big.