Summer High School 2009
Aaron Bertram

6. Euler's Formula. This formula and Fermat's Little Theorem (which is not to be confused with Fermat's Last, which is not little!) are easy to prove and have some very important practical consequences. Here it is:

Euler's Formula: If $n > 1$ and m is relatively prime to n, then:

$$m^{\phi(n)} \equiv 1 \bmod n$$

In particular, if $n = p$ is *prime*, then we get *Fermat's Little Theorem*:

$$m^{p-1} \equiv 1 \bmod p \text{ for all } m < p$$

Proof: Here's a quick proof of this pretty little theorem. Suppose:

$$m_1, m_2, m_3, \cdots, m_{\phi(n)}$$

are all the numbers from 1 to $n-1$ that are relatively prime to n. Then we can multiply each of them by m and take remainders to get:

$$(mm_1), (mm_2), (mm_3), \cdots, (mm_{\phi(n)}) \bmod n$$

which is also a list (in a different order) of exactly the *same* remainders. We know they are the same list because we could multiply them by the (mod n) reciprocal $1/m$ to get back the original list! Since they are the same remainders, we know that their product is the same (mod n). That is:

$$(mm_1) \cdot (mm_2) \cdots (mm_{\phi(n)}) \equiv m_1 \cdot m_2 \cdots m_{\phi(n)} \bmod n$$

Now we can multiply both sides by the product of the reciprocals $(1/m_1)(1/m_2)\cdots(1/m_{\phi(n)})$ to eliminate the list entirely, leaving:

$$m^{\phi(n)} \equiv 1 \bmod n$$

as desired. □

Examples:

(a) (Mod 2) $\phi(2) = 1$.

$$1^1 = 1$$

(b) (Mod 3) $\phi(3) = 2$.

$$1^2 = 1, \quad 2^2 = 4 \equiv 1$$

(c) (Mod 4) $\phi(4) = 2$.

$$1^2 = 1, \quad 3^2 = 9 \equiv 1$$

(d) (Mod 5) $\phi(5) = 4$.

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

(e) (Mod 6) $\phi(6) = 2$.

$$1^2 = 1, \quad 5^2 = 25 \equiv 1$$

(f) (Mod 10) $\phi(10) = 4$.

$$1^4 = 4, \quad 3^4 = 81 \equiv 1, \quad 7^4 = 2401 \equiv 1, \quad 9^4 = 6561 \equiv 1$$

Remember: This only applies when m and n are relatively prime!

We'll investigate here its use as a test for compositeness.

Corollary. Suppose $n > 1$ and:

$$m^{n-1} \not\equiv 1 \bmod n$$

for some m between 1 and $n - 1$. Then n is definitely composite.

Warning. This does **not** say that if some m (like, say, $m = 2$) gives $m^{n-1} \equiv 1 \bmod n$, then n is prime. It is inconclusive in that case. (On the other hand, this comes tantalizingly close to being true!)

Prime Search (Version 1): Which composite odd numbers between 3 and 30 can be proven to be composite by taking $m = 2$ and applying the Corollary? (We already know what we get for primes). If this seems stupid, remember that we are looking for a method to attack very large numbers. Also notice that the test tells us a number is composite *without telling us how to factor it!*

(Mod 9) $2^8 = 256 \equiv 4$. Composite.

(Mod 15) $2^{14} = 16384 \equiv 4$. Composite.

(Mod 21) $2^{20} = 1048576 \equiv 4$. Composite.

(Mod 25) $2^{24} = 16777216 \equiv 16$. Composite.

(Mod 27) $2^{26} = 67108864 \equiv 13$. Composite.

It detected all the composite numbers! (It works for even numbers, but this is for an obvious reason...try it!). It has the apparent drawback, however, of requiring one to compute ridiculously large numbers to test the compositeness of small numbers. This can be overcome with a clever use of modular and binary arithmetic. Oh, and by the way, the first composite number that is *not* detected by this most primitive of tests is $341 = 11 \cdot 31$, but 2^{340} has 148 digits, so we need to deal with the large number problem now.

Binary (Base 2): Remember that we can express every whole number in Binary as a string of zeroes and ones, with the kth digit (starting from the right) standing for the number (0 or 1) of kth powers of 2 we need when we write n as a sum of powers of 2.

Examples

(0) Counting in Binary: $1, 10, 11, 100, 101, 110, 111, 1000$, etc.

(1) 101011 (Binary) is $1 + 2 + 2^3 + 2^5 = 43$ (Base 10).

(10) Mersenne primes in Binary are exactly the primes of the form:

$$1111 \cdots 111 \text{ with a prime number of digits}$$

Conversion to Binary is very fast. To express n in Binary, just:

(i) If $n = 0$, STOP. Else if n is even, tack 0 to the left of the number. Otherwise, tack 1 to the left and subtract 1 from n.

(ii) Divide n by 2 and REPEAT.

Example: Convert 94 to Binary:

Rightmost digit: 0, change n to 47. Number so far: 0

Next digit: 1, change to 23. Number so far: 10

Next digit: 1, change to 11. Number so far: 110

Next digit: 1, change to 5. Number so far: 1110

Next digit: 1, change to 2. Number so far: 11110

Next digit: 0, change to 1. Number so far: 011110.

Next digit: 1, change to 0. Number so far: 1011110.

STOP.

Now that we can convert large numbers quickly into Binary, we are ready to take large powers mod n by:

The Method of Successive Squares: To compute the remainder for:

$$m^k \mod n$$

Step 1: Express k in Binary. Let l be the largest power of 2 that occurs.
Step 2: For i from 1 to l, compute m^{2^i} (and store it) by noticing that:

$$m^{2^{i+1}} = (m^{2^i})^2$$

so each one is the square of the previous, *which you may reduce mod* n.
Step 3: Multiply the appropriate powers together, according to the Binary form for k. (Keep reducing mod n to keep the numbers small.)

Example: We'll figure out 2^{340} mod 341 to check that it is a fake prime.

$$340 \text{ is } 101010100 \text{ in Binary}$$

or, in other words,

$$340 = 2^8 + 2^6 + 2^4 + 2^2$$

so

$$2^{340} = 2^{2^8} \cdot 2^{2^6} \cdot 2^{2^4} \cdot 2^{2^2}$$

and mod 341:

$$2^{2^0} = 2,\ 2^{2^1} = 4,\ 2^{2^2} = 16,\ 2^{2^3} = 256,\ 2^{2^4} = 65536 \equiv 64,$$

$$2^{2^5} \equiv 4096 \equiv 4,\ 2^{2^6} \equiv 16,\ 2^{2^7} \equiv 256,\ 2^{2^8} \equiv 64$$

so indeed:

$$2^{340} \equiv (64) \cdot (16) \cdot (64) \cdot (16) \equiv 1 \bmod 341$$

Notice: The largest numbers one ever has to see with this method are less than n^2, which are then reduced mod n (and if you are clever with minus signs, you can get away with numbers no bigger than $n^2/4$).

Example: So 341 fails the test for $m = 2$. Let's try $m = 3$. Mod 341:

$$3^{2^0} = 3,\ 3^{2^1} = 9,\ 3^{2^2} = 81,\ 3^{2^3} = 6561 \equiv 82,\ 3^{2^4} \equiv 6724 \equiv 245$$

$$3^{2^5} \equiv (245)^2 \equiv 9,\ 3^{2^6} \equiv 81,\ 3^{2^7} \equiv 82,\ 3^{2^8} \equiv 245$$

so

$$3^{340} \equiv (245) * (81) * (245) * (81) \equiv 56 \bmod 341$$

This proves that 341 is composite.