Chapter 8

Fermat's Little Theorem

8.1 Lagrange's Theorem

Let us recall (without proof) this basic result of group theory: *If G is a finite group of order n then*

$$g^n = 1$$

for all $g \in G$.

If G is commutative (as all the groups we consider will be) there is a simple way of proving this: Let

$$G = \{g_1, \ldots, g_n\}.$$

Then

$$\{gg_1, gg_2, \ldots, gg_n\}$$

are the same elements, in a different order (unless $g = 1$). Multiplying these elements together:

$$(gg_1)(gg_2)\cdots(gg_n) = g_1 g_2 \cdots g_n,$$

ie

$$g^n(g_1 g_2 \cdots g_n) = (g_1 g_2 \cdots g_n).$$

Multiplying by $(g_1 g_2 \cdots g_n)^{-1}$,

$$g^n = 1.$$

8.2 Euler's Theorem

Theorem 8.1 (Euler's Theorem)**.** *For all x coprime to n,*

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

Proof. The group $(\mathbb{Z}/n)^\times$ has order $\phi(n)$. The result follows on applying Lagrange's Theorem. □

8.3 Fermat's Little Theorem

As a particular case of Euler's Theorem, since $\phi(p) = p - 1$ if p is prime, we have

Theorem 8.2 (Fermat's Little Theorem)**.** *If p is prime then*

$$x^{p-1} \equiv 1 \bmod p$$

for all x coprime to p.

The title 'Fermat's Little Theorem' is sometimes given to the following variant.

Corollary 8.1. *If p is prime then*

$$x^p \equiv x \bmod p$$

for all x.

Proof. If $p \nmid x$ the result follows on multiplying the congruence in the Theorem by x. If $p \mid x$ then trivially $x^p \equiv 0 \equiv x \bmod p$. □

8.4 Carmichael numbers

Fermat's Little Theorem suggests a simple test for the primality of n: *Is $x^n \equiv x \bmod n$ for all x?*

This is sometimes known as Fermat's Primality Test.

Example: Take $n = 6$, for example. The congruence obviously holds for $x = 0, 1$. But for $x = 2$,

$$2^6 = 64 \equiv 4 \bmod 6,$$

so the test fails, and we have proved that 6 is not prime.

Unfortunately, it turns out that some composite numbers can satisfy Fermat's test for all x.

Definition 8.1. *We say that $n \in \mathbb{N}$ is a* Carmichael number *if n is composite but*

$$x^n \equiv x \bmod n \text{ for all } x.$$

Example: The smallest Carmichael number is

$$561 = 3 \cdot 11 \cdot 17.$$

To see that 561 is a Carmichael number, note that $3 - 1 = 2, 11 - 1 = 10$ and $17 - 1 = 16$ all divide $561 - 1 = 560$.

Suppose first that x is coprime to 561. By Fermat's Little Theorem,

$$x^2 \equiv 1 \bmod 3 \implies x^{560} \equiv 1 \bmod 3$$

Similarly,

$$x^{10} \equiv 1 \bmod 11 \implies x^{560} \equiv 1 \bmod 11,$$
$$x^{16} \equiv 1 \bmod 17 \implies x^{560} \equiv 1 \bmod 17.$$

Putting these together, we deduce that

$$x^{560} \equiv 1 \bmod 3 \cdot 11 \cdot 17 = 561 \implies x^{561} \equiv x \bmod 561.$$

But what if x is not coprime to 561, say $17 \mid x$ but $3, 11 \nmid x$? Then

The congruence is trivially satisfied mod 17:

$$(17y)^{561} \equiv 17y \bmod 17.$$

So we only have to show that

$$(17y)^{561} \equiv 17y \bmod 33,$$

Now $\phi(33) = 2 \cdot 10 = 20$. Since 17 and y are coprime to 33, it follows by Euler's Theorem that

$$17^{20} \equiv 1 \bmod 33 \text{ and } y^{20} \equiv 1 \bmod 33.$$

Hence

$$\begin{aligned}(17y)^{20} \equiv 1 \bmod 33 &\implies (17y)^{560} \equiv 1 \bmod 33 \\ &\implies (17y)^{561} \equiv 17y \bmod 33.\end{aligned}$$

The other cases where x is divisible by one or more of $3, 11, 17$ can be dealt with similarly.

We shall prove the following result later. The argument is similar to that above, but requires one more ingredient, which we shall meet in the next Chapter.

Proposition 8.1. *The number n is a Carmichael number if and only if it is square-free, and*

$$n = p_1 p_2 \cdots p_r$$

where $r \geq 2$ and

$$p_i - 1 \mid n - 1$$

for $i = 1, 2, \ldots, r$.

There are in fact an infinity of Carmichael numbers — this was only proved about 20 years ago — although they are sparsely distributed. (There are about $N^{1/3}$ Carmichael numbers $\leq N$.)

Note that if a number fails Fermat's test then it is certainly composite. The converse is not true, as we have seen; a number may pass the test but not be prime.

However, Fermat's test does provide a reasonable *probabilistic* algorithm, for determining "beyond reasonable doubt" if a large number n is prime: Choose a random number $x_1 \in [2, n-1]$, and see if

$$x_1^n \equiv x_1 \bmod n.$$

If this holds, then the chances of n being prime are certainly much better than they were before. Far fewer than $1/2$ of composite numbers satisfy this congruence. So one could say that the odds of the number being prime are at least doubled.

Now repeat the test with a second random number $x_2 \in [2, n-1]$ and repeat the test. There is no reason to suppose that there is any statistical relation between the two tests; so if the test is passed again, the chances of the number being prime are at least 4 times as great.

If we repeat the test 20 times, say, and n passes each time, we may say that the number is "virtually certain" to be prime.

Having said all that, Fermat's test is never used in practice, because there is a simple variant which avoids the Carmichael number problem, and has other advantages as well.

8.5 The Miller-Rabin test

Suppose p is an odd prime. Let

$$p - 1 = 2^e m,$$

where m is odd.

Suppose $p \nmid x$. Then we know that

$$x^{p-1} = x^{2^e m} \equiv 1 \bmod p.$$

But this may be written

$$\left(x^{2^{e-1}m}\right)^2 \equiv 1 \bmod p.$$

It follows that

$$x^{2^{e-1}m} \equiv \pm 1 \bmod p;$$

for $\mathbb{Z}/(p)$ is a field; so if $x \in \mathbb{Z}/(p)$ then

$$x^2 = 1 \implies (x-1)(x+1) = 1 \implies x = \pm 1$$

Now suppose

$$x^{2^{e-1}m} \equiv 1 \bmod p.$$

Then we can repeat the argument, if $e > 1$, to see that

$$x^{2^{e-2}m} \equiv \pm 1 \bmod p.$$

Continuing in this way, we see that either

$$x^{2^i m} \equiv -1 \bmod p$$

for some $i \in [0, e-1]$. or else

$$x^m \equiv 1 \bmod p.$$

That is the Miller-Rabin test. It turns out that if a number n passes the test for all x coprime to n then it must be prime; there is no analogue of Carmichael numbers.

But we shall need the results of the next chapter to establish this ....

8.6 The AKS algorithm

The Miller-Rabin test (like the Fermat test) is *probabilistic*. It will only determine *up to a given probability* if a number is prime. Just over 10 years ago, three Indian mathematicians — Agrawal, Kayal and Saxena — found a deterministic polynomial-time primality algorithm.

This algorithm is based on a simple extension of Fermat's Little Theorem to polynomias.

Theorem 8.3. *The integer $n \geq 2$ is prime if and only if*

$$(x + a)^n \equiv x^n + a \bmod n$$

for all a.

Remark: Suppose $f(x) = \sum a_i x^i$, $g(x) = \sum b_i x^i \in \mathbb{Z}[x]$. We say that $f(x) \equiv g(x) \bmod n$ if $a_i \equiv b_i \bmod n$ for all i.

Lemma 8.1. *If p is prime then*

$$p \mid \binom{i}{p}$$

for $i \neq 0, p$.

Proof. We have

$$\binom{i}{p} = \frac{p(p-1)\cdots(p-i+1)}{i(i-1)\cdots 1}.$$

The only term divisible by p is the first term in the numerator. □

It follows from this lemma that the relation in the theorem holds if n is prime.

Suppose n is not prime, say $p^i \parallel n$ where p is prime. Then

$$p^{i-1} \parallel \binom{n}{p}.$$

For

$$\binom{n}{p} = \binom{n}{n-p} = \frac{n(n-1)\cdots(n-p+1)}{p(p-1)\cdots 1}.$$

The first term in the numerator is divisible by p^i, and the first term in the numerator is divisible by p. The result follows, since no other terms are divisible by p. □

It is not clear at this point that this result improves on the Miller-Rabin test, since it is not feasible to test the relation for all $a \in (0, n)$. However, the AKS trio showed that it is only necessary to test

$$0 < a \leq \sqrt{\phi(r)}\log_2 n,$$

where r is the smallest positive integer such that the order of $r \mod n$ is $> (\log_2 n)^2$. The trio showed that $r < (\log_2 n)^5$, thus establishing that the algorithm can be completed in polynomial time; that is, in $\leq P(\log_2 n)$ steps, where $P(x)$ is a polynomial.