THE EULER-FERMAT THEOREM AND RSA CRYPTOGRAPHY

Fermat's Little Theorem states that, for every integer x and every prime p, the number $x^p - x$ is divisible by p. Equivalently, for a prime p and an integer x which is not divisible by p, the difference $x^{p-1} - 1$ is divisible by p. This last statement is clear as the remainder of x modulo p is nonzero, that is, lies in the $(p-1)$-element multiplicative group $\mathbf{Z}_p \setminus \{0\}$, and so its $(p-1)$th power in that group equals 1.

A more general statement is the *Euler-Fermat Theorem*, which uses the function ϕ assigning to every positive integer n the number of those positive integers which are less than n and relatively prime to n, so that $\phi(p) = p - 1$ if and only if p is a prime or $p = 1$. It states that, for every positive integer n and every integer x relatively prime to n, the difference $x^{\phi(n)} - 1$ is divisible by n. In fact, the remainder of x modulo n is not a zero divisor in the ring $\mathbf{Z}_n$, and hence, as $\mathbf{Z}_n$ is finite, it is invertible, and our assertion follows since the multiplicative group of all invertible elements of $\mathbf{Z}_n$ has $\phi(n)$ elements.

Finally, let an integer $n = pq$ be the product of two different primes p, q, so that $\phi(n) = (p-1)(q-1)$. Also, let a, b be positive integers whose remainders modulo $\phi(n)$ are invertible in $\mathbf{Z}_{\phi(n)}$ and form each other's inverses. Then, for every integer x, the number $x^{ab} - x$ is divisible by n. In fact, $ab = 1 + s\phi(n)$ for some nonnegative integer s, and all we need to verify is that multiplying x by $x^{\phi(n)}$ modulo n we still get x modulo n (so that x multiplied by the sth power of $x^{\phi(n)}$ remains x, modulo n, and $x^{ab} \equiv x$ modulo n, as required). However, when x is relatively prime to $n = pq$, this is clear from the Euler-Fermat Theorem; when x is divisible by $n = pq$, it is trivial; in the remaining case, switching the symbols p, q if necessary we may assume that x is divisible by q and not by p, so that Fermat's Little Theorem (applied to x^{q-1} (rather than x) and p gives $(x^{q-1})^{p-1} = 1 + kp$ for some nonnegative integers k, and $x \cdot x^{\phi(n)} - x = x[x^{(p-1)(q-1)} - 1] = kpx$, which is divisible by $n = pq$, since x is divisible by q.

This leads to the following procedure of *RSA cryptography*. We choose two large different primes p, q, so large that even modern supercomputers are unable to factorize $n = pq$. We also choose a, b as above, and make the values of n and a *public* (that is, we announce them to everyone interested). Anybody sending us a message, which is an element x of $\mathbf{Z}_n$, encodes it first by raising x to the ath power in $\mathbf{Z}_n$, and then sends us the result, y. To decode it, we raise y to the bth power in $\mathbf{Z}_n$, obtaining x. Others cannot find b, which is the inverse of a modulo $\phi(n) = (p-1)(q-1)$, and they do not know what p and q are.

Another useful application of this procedure is *authentication of signatures*. Suppose that we send a message to another recipient, using that recipient's analogues of our n and a (which are a matter of public record). In addition, we include a "signature", identifying us as the sender (possibly with the date, etc., so that no one could intercept it and then use it to impersonate us on later occasions). That signature is some element z of $\mathbf{Z}_n$ (our n) and we encode it by raising it to the bth power in $\mathbf{Z}_n$. The recipient only needs to raise that bth power to the ath power in $\mathbf{Z}_n$ (and everyone knows what our n, a are), which yields our original signature z.