A property dealing with the order of 3 modulo a Mersenne prime

Tony Reix (tony.reix@laposte.net)

ZetaX (AOPS forum)

2008, 8th of March

In May of 2006, based on experimental data I provided, ZetaX (his "User-Name" on the *Art of Problem Solving* and *Mathlinks* Maths forums) proved the following theorem:

Theorem 1 (ZetaX)

$$order(3, M_q) = 2\ [\ \eta(3, M_q) - 1\ ]\ .$$

1 Definitions

$\eta(b, N)$ is the number of distinct numbers $b^n + 1/b^n \pmod{N}$.

$order(b, N)$ is the least n such that $b^n \equiv 1 \pmod{N}$.

$M_q = 2^q - 1$ is a Mersenne prime.

2 Proof by ZetaX

Let p be any odd prime. And let $f(x) := x + \frac{1}{x} \pmod p$.
Then we want the size (lets call it: $\eta(k,p)$) of the set $\{f(k^n) \mid n \in \mathbb{N}\}$.

First lets find out how often $f(x) \equiv f(y) \pmod p$ with $x, y \not\equiv 0 \pmod p$ happens. This means: $x + \frac{1}{x} \equiv y + \frac{1}{y} \pmod p \iff x^2y + y \equiv xy^2 + x \pmod p \iff (xy-1)(x-y) \equiv 0 \pmod p$. This means that either $x \equiv y \pmod p$, the trivial case, or $xy \equiv 1 \pmod p$. But, when $x \equiv \pm 1 \pmod p$, then only the case $x \equiv y \pmod p$ can occur.

Look at the set $\mathrm{Pow}(k) := \{k^n \pmod p \mid n \in \mathbb{Z}\}$ (we can use $\mathbb{Z}$ instead of $\mathbb{N}$ because of Fermat's Little Theorem). It has size $|\mathrm{Pow}(k)| = ord(k,p)$.
Additionally, we can pair up the elements $k^n \pmod p$ and $k^{-n} \pmod p$ for each n, since they give the same value $f(k^n) \equiv f(k^{-n}) \pmod p$, and only those are equal (note that $1, -1 \pmod p$ will be left alone, but each noted as "pair" with one element).

Since different pairs give different values, we have: $\eta(k,p) =$ *number of such pairs.*

Thus when $-1 \in \mathrm{Pow}(k)$ (1 is always in the set), there will be $\frac{ord(k,p)-2}{2} + 2 = \frac{ord(k,p)+2}{2}$ pairs, thus by the above: $\eta(k,p) = \frac{ord(k,p)+2}{2} \iff 2\eta(k,p) = ord(k,p) + 2$.
Similar when -1 is not in the set: $2\eta(k,p) = ord(k,p) + 1$.

This for example gives $\eta(3,7) = 4$.

To find out if -1 is in the set, we need to know if the order of $k \pmod p$ is even or odd (this suffices to know: when $ord(k,p)$ would be odd, we couldn't have $2\eta(k,p) = ord(k,p) + 2 \pmod 2$, and analogous for the other case).

When s is the biggest integer with $2^s \mid p-1$, we could calculate $k^{\frac{p-1}{2^s}} \pmod p$ (since $\frac{p-1}{2^s}$ is the biggest odd divisor of $p-1$) and look if it is $1 \pmod p$ or not (the order is odd iff it is $1 \pmod p$).
When $4 \nmid p-1$, we just ask whether k is a quadratic residue $\pmod p$ or not, which can be checked by Jacobi symbols.

Special case $k = 3$ and $p = 2^q - 1$: then $4 \nmid p-1$. Thus we use Legendre symbols (Jacobi is not needed since both numbers are prime) and the law of quadratic reciprocity: $\left(\frac{3}{2^q-1}\right) = -\left(\frac{2^q-1}{3}\right) = -1$. This shows that the order of $3 \pmod p$ is even.

Thus for Mersenne primes $p = M_q$, it is: $2\eta(3,p) = ord(3,p) + 2$. $\square$