

Theorem 1 (Robert Gerbicz) *Let $q > 3$ prime and $p = W(q) = \frac{2^q+1}{3}$ is also prime (Wagstaff prime), then for the sequenc $S_0 = \frac{3}{2}$, $S_{k+1} = S_k^2 - 2$ it is true that $S_q - S_1$ is divisible by p .*

It is the same as the original conjecture for $U_0 = \frac{1}{4}$, $U_{k+1} = U_k^2 - 2$, because in our sequence $S_1 = U_0$ and the recursion is the same, so $U_{q-1} - U_0 = S_q - S_1$.

It is known that $T = Q[\sqrt{-7}] = Q[\sqrt{7} * I]$ is a prime factorization field. First I prove:

Lemma: Suppose that p is an odd positive prime in Z , different from 7, a and b are integers in Z , let $z = \frac{a+b\sqrt{7}*I}{4}$ then if $(\frac{-7}{p}) = 1$ and $gcd(z, p) = 1$ then $z^{p-1} \equiv 1 \pmod{p}$. If $(\frac{-7}{p}) = -1$ then $z^{p+1} \equiv norm(z) \pmod{p}$.

Proof: use Fermat's little theorem and that binomial(p,k) is divisible by p if $0 < k < p$.

$$(4z)^p \equiv 4^p z^p \equiv 4z^p \pmod{p}$$

$$(4z)^p \equiv (a+b\sqrt{7}I)^p \equiv a^p + b^p \sqrt{7}^p I^p \equiv a + b7^{\frac{p-1}{2}} \sqrt{7}(-1)^{\frac{p-1}{2}} I \equiv a + b(\frac{-7}{p})\sqrt{7}I \pmod{p}$$

so $4z^p \equiv 4z$ or $4\bar{z} \pmod{p}$.

First part: let $(\frac{-7}{p}) = 1$ then we can write: $4z^p \equiv 4z \pmod{p}$ if $gcd(z, p) = 1$ then $z^{p-1} \equiv 1 \pmod{p}$.

Second part: let $(\frac{-7}{p}) = -1$ then $4z^p \equiv 4\bar{z} \pmod{p}$, multiple this by z , we get: $4z^{p+1} \equiv 4norm(z) \pmod{p}$, so $z^{p+1} \equiv norm(z) \pmod{p}$ is also true.

Proof of the lemma is complete.

Proof of the theorem 1: Let $\omega = \frac{3+\sqrt{7}I}{4}$ an element in the field. Let $S_0 = \frac{3}{2}$ and $S_{k+1} = S_k^2 - 2$, by induction it is easy to see, that $S_k = \omega^{2^k} + \bar{\omega}^{2^k}$, for this use that $norm(\omega) = 1$

If $q > 3$ prime then $q = 6k + 1$, so $p = W(q) = \frac{2^q+1}{3} \equiv 11$ or $15 \pmod{28}$, using this we can get that $(\frac{-7}{p}) = 1$. Use the lemma for $z = \omega$ and for $p = W(q)$ prime, we obtain:

$$\omega^{W(q)-1} \equiv 1 \pmod{p}$$

$$\omega^{\frac{2^q-2}{3}} \equiv 1 \pmod{p} \text{ raise it to cube:}$$

$$\omega^{2^q-2} \equiv 1 \pmod{p} \text{ multiple it by } \omega^2$$

$$\omega^{2^q} \equiv \omega^2 \pmod{p}, \text{ conjugate it:}$$

$$\bar{\omega}^{2^q} \equiv \bar{\omega}^2 \pmod{p} \text{ Adding these two lines: } S_q = \omega^{2^q} + \bar{\omega}^{2^q} \equiv \omega^2 + \bar{\omega}^2 = S_1 \pmod{p}, \text{ so } S_q - S_1 \text{ is divisible by } p, \text{ proof is complete.}$$

Theorem 2 (Robert Gerbicz) *Let $S_0 = -\frac{3}{2}$ and $S_{k+1} = S_k^2 - 2$ sequence. If $p = F(n) = 2^{2^n} + 1$ is a Fermat prime then $S_{2^n} - S_1$ is divisible by p .*

This is almost the original conjecture (that was: $S_{2^n-1} - S_0$ is divisible by p).

Proof of the theorem 2:

For $n = 0$ it is true. Now suppose that $n > 0$ and replace S_0 by $-S_0$, and by this we get the same sequence for S_k , if $k > 0$. But this sequence is the same as the S sequence was for the Wagstaff primes. $p = F_n \equiv 5$ or $17 \pmod{28}$, using this it is easy to see, that $\left(\frac{-7}{p}\right) = -1$, $norm(\omega) = 1$, $gcd(norm(\omega), p) = gcd(1, p) = 1$, using the lemma:

$$\omega^{p+1} \equiv 1 \pmod{p}$$

$$\omega^{2^{2^n}+2} \equiv 1 \pmod{p}, \text{ multiple it by } \bar{\omega}^2$$

$$\omega^{2^{2^n}} \equiv \bar{\omega}^2 \pmod{p}, \text{ conjugate it:}$$

$$\bar{\omega}^{2^{2^n}} \equiv \omega^2 \pmod{p}$$

Add the two lines: $S_{2^n} = \omega^{2^{2^n}} + \bar{\omega}^{2^{2^n}} \equiv \bar{\omega}^2 + \omega^2 = S_1 \pmod{p}$. So $S_{2^n} - S_1$ is divisible by p . The proof is complete.