A really trivial proof for proving Wagstaff numbers prime.

Anton Vrba

October 8, 2008

Abstract

It is now possible to prove Wagstaff numbers, of the form $W_p = \frac{1}{3}(1+2^p)$, prime! Proof for a test is based on properties of groups and of the iteration $s \to s^2 - 2$. Primality is given if the result of the second iteration equals the result of the p^{th} iteration.

Revision: 2.0 e-mail: antonvrba@gmail.com

Theorem 1 :(Vrba)
Let $S_{n+1} = S_n^2 - 2$ and p be prime larger than 3. $W_p = \frac{1}{3}(1+2^p)$ is prime if and only if $S_p = S_2 \pmod{W}_p$ where $S_0 = 6$
or as an alternative $S'_p = S'_1 \pmod{W}_p$ where $S'_0 = 2^{(p-2)}$

Proof of necessity:
The proof uses the same arguments of the proof that Bruce(1993)[*1)] used to prove the Lucas-Lehmer test for Mersenne primes. His proof makes use of the following Lemma. If G is a finite group then the order of an element is at most the order of the group. If $x \in G$ and $x^r = 1$ then the order of x divides r.

To prove Wagstaff numbers prime on the basis of Bruce, said Lemma needs to be adapted, with this we start.

Lemma 1 Let $G_{\sqrt{c}}(p)$ be a finite group of elements of elements $a+b\sqrt{c}$, α and β be the roots of $x^2 - ax + 1 = 0$ and we have, by some or other calculation, derived two equalities $\alpha^{2^p-2n} - 1 = 0$ and $\alpha^{2^{p-1}-n} + 1 = 0$ we can conclude that the order of the element $a + b\sqrt{c}$ is a multiple of 2^p

Proof: We do a step for step analysis of the possible ways to define the order of an element of type integer, Gaussian integer and of form $a + b\sqrt{c}$ in a finite group.

If G is a finite group then the order of an element is at most the order of the group.

If $x \in G$ and $x^r = 1$ then the order of x divides r. If $x^s = -1$ then the order of x is $2s$ if and only if $2s = r$.

Now consider the group $G_c(p)$ of Gaussian integers, it has p^2 elements, Let $p = 2k + 1$ and k odd then $(a + Ib)^i \neq 1$ for all i, then if $(a + Ib)^r =$

$(a + Ib)$ and if $(a + Ib)^s = (a - Ib)$ then the order of x is $2s$ if and only if $2s = r$. Let $p = 2k + 1$ and k even, then if $(a + Ib)^r = 1$ and if $(a + Ib)^s = -1$ then the order of $a + Ib$ is $2s$, if and only if $2s = r$.

To continue the reasoning now consider the group $G_{\sqrt{c}}(p)$ of elements $a + b\sqrt{c}$, presume the multiplicative operation within the group is such that $(a + b\sqrt{c})^r = (a + b\sqrt{c})^{2n}$ and $(a + b\sqrt{c})^s = (a - b\sqrt{c})^n$ then the minimum order of $a + b\sqrt{c}$ is $2s$ if and only if $2s = r$. The same applies for the element $(a + Ib\sqrt{c})$.

Therefore the derived equalities $\alpha^{2^r+2n} - 1 = 0$ and $\alpha^{2^s+n} + 1 = 0$ are interpreted in the group as

$\alpha^{2^p-2n} - 1 = 0$ is written as $\alpha^{2^p} = \alpha^{2n}$

$\alpha^{2^{p-1}-n} + 1 = 0$ is written as $\alpha^{2p-1} = \bar{\alpha}^n$

and by above reasoning the minimum order of the element α is 2^p

This concludes the proof of Lemma 1.

Given $a \in G(p)$(the finite field with p elements), lets define the polynomial $u(X) = X^2 - aX + 1$. Let α and β be the roots of u in $G(p^2)$. Note that $\alpha + \beta = a$ and $\alpha\beta = 1$.

Lemma 2: We have $h^n(a) = \alpha^n + \beta^n$ for $n > 0$.

Proof. By induction on n. For $n = 0$ we have $h^0(a) = a = \alpha + \beta$ assume the result is true for n; we prove it for $n + 1$. We have:

$\alpha^{2^{n+1}} + \beta^{2^{n+1}} = (alpha^{2^n} + \beta^{2^n})^2 - 2\alpha^{2^n}\beta^{2^n} = h^n(a)^2 - 2.$

The test condition of the theorem is $S_p = S_2 \pmod{W}_p$ which means that:

(1.1) $h^p(6) - h^2(6) = 0$

It is true that $S_2 = S_1^2 - 2$ and $S_2 = (-S_1)^2 - 2$ and $S_p = (S_{p-1})^2 - 2 = S_2$ therefore we can write the second identity

(1.2) $h^{p-1}(6) + h^1(6) = 0$

By the Lemma 2 (1.1) is equivalent to

$\alpha^{2^p} + \alpha^{-2^p} - \alpha^{2^2} - \alpha^{-2^2}$

multiplying by α^{2^p} results in $\alpha^{2^{p+1}} + 1 - \alpha^{2^p+2^2} - \alpha^{2^p-2^2}$ which factors $(\alpha^{2^p} - \alpha^{2^2})(\alpha^{2^p} - \alpha^{-2^2}) = 0$ and we can write the following equalities:

(1.3) $\alpha^{2^p-4} - 1 = 0$ or $\alpha^{2^p+4} - 1 = 0$

Similarly (1.2) is equivalent to:

$(\alpha^{2^{p-1}} + \alpha^{2^1})(\alpha^{2^{p-1}} + \alpha^{-2^1}) = 0$ and we can write the following equalities

(1.4) $\alpha^{2^{p-1}-2} + 1 = 0$ or $\alpha^{2^{p-1}+2} + 1 = 0$

(In Theorem 12 of Vasiga and Shallit (2003)*2 demonstrated the elegant way how to express identity (1.1) in terms of α which was also applied to the new identity (1.2), both which are necessary to define the order of α a prerequisite to continue with the proof)

The result (1.3) and (1.4) essentially concludes the proof as the exact same reasoning presented by Bruce follows from here but using the results from above.

As (1.3) and (1.4) are modula W_p we write them more explicitly by replacing the zero wit RW_p for some integer R.

(1.5) ; $\alpha^{2^p-4} = RW_p + 1$ or $\alpha^{2^p+4} = RW_p + 1$

(1.6) ; $\alpha^{2^{p-1}-2} = RW_p - 1$ or $\alpha^{2^{p-1}+2} = RW_p - 1$

From now on quoting Bruce word for word I bring the proof to its conclusion, for completeness of this document.

Lemma 2. Let X be a set with a binary operation which is associative and has an identity. Then the set X^* of invertible elements in X forms a group.

Proof: Clearly the identity $1 \in X^*$, so we have a non-empty set. We now have only to show that the set X^* is closed under the binary operation. But if x_1 and x_2 are invertible elements with inverses x_1^{-1}, x_2^{-1} then x_1x_2 has inverse $x_2^{-1}x_1^{-1}$.

Proof of Theorem 1: Let Z_q denote the set of integers modulo q, and X denote the set $\{a + b\sqrt{2} \ : \ a, b \in Zq\}$. We can define two binary operations on X, namely addition and multiplication, in the obvious manner. So in the case of multiplication, which is the one of interest, we choose representatives in $Z[\sqrt{2}]$ of our elements of X compute the product in the usual way, $(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})$ as $(a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$ and then reduce the coefficients modulo q. In the case of addition we obviously get an abelian group, and for multiplication we clearly have an associative (and commutative) binary operation with identity 1. Let X^* denote the group of invertible elements of X with respect to multiplication. Lemma 3 tells us that this is a group, while Lemma 1 tells us that the order of any element of X^* is at most $q^2 - 1$, since X^* contains at least one non-invertible element, namely 0. Now consider $\alpha = 3 + 2\sqrt{2}$ as an element of X. Since q divides W_p it follows that RW_p, when viewed as an element of X, is 0. So the equalities noted in (1.5) and (1.6) above in X reduce to

$\alpha^{2^{p-4}-4} = 1$ or $\alpha^{2^{p+4}+4} = 1$

$\alpha^{2^{p-1}-2} = -1$ or $\alpha^{2^{p-1}+2} = -1$

respectively. It follows that α lies in X^*, and from Lemma 1 has order 2^p. For the order of α clearly divides 2^p using Lemma 1 and the first equality, but cannot be less than (2^p) by the second. So using Lemma 1 again we deduce that $(2^p) < q^2 - 1$. However $q^2 - 1 < W_p - 1 = \frac{1}{3}(2^p + 1)$ and we have a contradiction.

End of of prove of necessity.

Proof of sufficiency:

Let $S_0 = \alpha + \beta$ with $\alpha = (3 + 2\sqrt{2})$ and $\beta = (2 + 2\sqrt{2})$

If $W_p = \frac{1}{3}(1 + 2^p)$ is prime we can proceed as follows:

$(\alpha)^{W_p} = (3^{W_p} + ... + (2)^{\frac{W_p - 1}{2}}\sqrt{2})$

$\alpha^{\frac{1+2^p}{3}} \equiv 3 + \left(\frac{2}{W_p}\right)\sqrt{2} \pmod{W_p}$ where $\left(\frac{2}{W_p}\right)$ is the Legendre symbol

$\left(\frac{2}{W_p}\right) = -1$ as $W_p \equiv 3 \pmod 8$

$\alpha^{\frac{1+2^p}{3}} \equiv 3 - 2\sqrt{2} = \beta \pmod{W_p}$

Multiply both sides by α, (remember $\alpha\beta = 1$), then cube both sides and finally multiply both sides by β^4

we obtain $\alpha^{2^p} \equiv \beta^{2^2} \pmod{W_p}$, similarly $\beta^{2^p} \equiv \alpha^{2^2} \pmod{W_p}$

and adding the two results completes the proof of sufficiency for $S_p = S_2 \pmod{W)_p}$

Thereby, completing the proof of the stated theorem!

As a consequence, new class of provable primes

This proof possibly opens the way to prove the following class of numbers prime. Below three forms already identified , the starting value followed by the test condition.

$V_{n3} = 2^n + 3,\ S_0 = 6\ S_n = S_2$

$V_{n5} = 2^n + 5,\ S_0 = 4\ S_n = S_2$

$V_{n7} = 2^n + 7,\ S_0 = 5\ S_n = S_3$

---

*1) J. W. Bruce, "A really trivial proof of the lucas-lehmer test," Amer. Math. Monthly, 100 (1993) 370-371.

*2) Troy Vasiga,Jeffrey Shallit, "On the iteration of certain quadratic maps over $GF(p)$"