A really trivial proof for proving Wagstaff numbers prime.

Anton Vrba

October 5, 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. The 'order of the group' is discussed briefly to show that the order of an element $\omega = a + b\sqrt{c}$ can be determined even though no solution $\omega^k = 1$ exist; the order can be evaluated if $\omega^n = \bar{\omega}^j$.

Revision: 0.0 e-mail: antonvrba@gmail.com

Theorem :(Vrba)
Let p be an odd prime larger than 3. $W_p = \frac{1}{3}(1+2^p)$ is prime if and only if

$S_p = S_2 (mod\ W_p)$
where $S_0 = 6$ and $S_{n+1} = S_n^2 - 2$

The proof uses the same final argument of the proof that Bruce(1993)[*1)] used to prove the Lucas-Lehmer test for Mersenne primes. It relies on the fact that the order of an element divides the order of the group. At this point I would like to discuss the term 'order of the group' and is normally defined as: The order of an element g of a finite group $\mathbf{G}$ is the smallest power of n such that $g^n \equiv 1$ and we write $\text{ORD}_G(g) = n$. But, consider an element $\omega = a + b\sqrt{c}$ that has no solution $\omega^k \equiv 1$ but has a solution $\omega^n \equiv \bar{\omega}$, thus the $\text{ORD}_G(\omega) = 2n$ and $\text{ORD}_G(\omega + \bar{\omega}) = n$. Further, if $\omega^n \equiv \bar{\omega}^j$, thus the $\text{ORD}_G(\omega) = 2(n-j+1)$ and $\text{ORD}_G(\omega + \bar{\omega}) = n - j + 1$. One can continue this argument for $\omega^{2n} \equiv -\bar{\omega}^2$, and taking the square root $\omega^n \equiv \mathtt{i}\bar{\omega}$ thus the $\text{ORD}_G(\omega) = 4n$ and $\text{ORD}_G(\omega + \bar{\omega}) = 2n$. This will be used at the end of the proof.

We separate the proof into two parts.
Proof of sufficiency:
(1) Let $S_0 = \omega + \bar{\omega}$ with $\omega = 3 + 2\sqrt{2}$ and $\bar{\omega} = 3 - 2\sqrt{2}$
then by induction $S_n = \omega^{2^n} + \bar{\omega}^{2^n}$
(2) If $W_p = \frac{1}{3}(1+2^q)$ is prime we can proceed as follows:

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

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

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

(6) $\omega^{\frac{1+2^q}{3}} \equiv 3 - 2\sqrt{2} = \bar{\omega} \pmod{W_p}$

Multiply both sides by ω, (remember $\omega\bar{\omega} = 1$), then cube both sides and finally multiply both sides by $\bar{\omega}^4$ we obtain

(7) $\omega^{2^p} \equiv \bar{\omega}^{2^2} \pmod{W_p}$. Similarly, $\bar{\omega}^{2^p} \equiv \omega^{2^2} \pmod{W_p}$

(8) and adding the two results completes the proof of sufficiency for $S_p = S_2(mod\ W_p)$.

Proof of necessity:

If $S_p = S_2(mod\ W_p)$ and iterating $s \to s^2 - 2$ it follows that:

(9) $S_{p-1} = -S_1(mod\ W_p)$

(10) Let $S_0 = \omega + \bar{\omega}$ with $\omega = 3 + 2\sqrt{2}$ and $\bar{\omega} = 3 - 2\sqrt{2}$

then by induction $S_n = \omega^{2^n} + \bar{\omega}^{2^n}$

(11a) $S_{p-1} = -S_1(mod\ W_p)$ means that $\omega^{2^{p-1}} + \bar{\omega}^{2^{p-1}} + \omega^2 + \bar{\omega}^2 \equiv 0 \pmod{W_p}$

and

(11b)$S_p = S_2(mod\ W_p)$ means that $\omega^{2^p} + \bar{\omega}^{2^p} \equiv +\omega^4 + \bar{\omega}^4 \pmod{W_p}$

and we can split (11a) into two parts:

(12a) $\omega^{2^{(p-1)}} + \omega^2 \equiv \delta \pmod{W_p}$

(12b) $\bar{\omega}^{2^{(p-1)}} + \bar{\omega}^2 \equiv -\delta \pmod{W_p}$

Multiplying (12a) by ω^2 and (12b) by $\bar{\omega}^2$ we obtain

(13a) $\omega^2\omega^{2^{(p-1)}} + \omega^4 \equiv \delta\omega^2 \pmod{W_p}$

(13b) $\bar{\omega}^2\bar{\omega}^{2^{(p-1)}} + \bar{\omega}^4 \equiv -\delta\bar{\omega}^2 \pmod{W_p}$

adding (13a) and (13b) and using (11b) to eliminate $\omega^4 + \bar{\omega}^4$ we get

(14) $\omega^2\omega^{2^{(p-1)}} + \omega^{2^p} + \bar{\omega}^2\bar{\omega}^{2^{(p-1)}} + \bar{\omega}^{2^p} = \delta(\omega^2 - \bar{\omega}^2) \pmod{W_p}$

which factors

(15) $\omega^{2^{(p-1)}}(\omega^2 + \omega^{2^{(p-1)}}) + \bar{\omega}^{2^{(p-1)}}(\bar{\omega}^2 + \bar{\omega}^{2^{(p-1)}}) = \delta(\omega^2 - \bar{\omega}^2) \pmod{W_p}$

and using (12a) and (12b) to cancel the δ

(16)$\omega^{2^{(p-1)}} - \bar{\omega}^{2^{(p-1)}} = \omega^2 - \bar{\omega}^2 \pmod{W_p}$

Adding (11a) to (16) we obtain

(17) $\omega^{2^{(p-1)}} = -\bar{\omega}^2 \pmod{W_p}$

and the square root on both sides

(18) $\omega^{2^{(p-2)}} = \mathtt{i}\bar{\omega} \pmod{W_p}$

hence the order of ω in $\mathbf{G} = \mathbf{Z}_{W_p}[\sqrt{2}]^*$ of all numbers $a + b\sqrt{2}$ which are invertible is:

$\text{ORD}_G(\omega) = 4 \times 2^{(p-2)} = 2^{(p-2)}$ and

(19)$\text{ORD}_G(\omega + \bar{\omega}) = 2 \times 2^{(p-2)} = 2^{(p-1)}$

Now, for proof by contradiction, assume W_p is composite and choose one of its prime divisors q that is not greater than its square root. Consider the group $G = \mathbf{Z}_q[\sqrt{2}]^*$ of all the numbers $(a + b\sqrt{2}) + (a - b\sqrt{2})$ modulo q which are invertible. Note G has at most $q^2 - 1$ elements. We know

from (19) that the $\omega + \bar{\omega}$ is an element of G with order $2^{(p-1)}$. Since the order of an element is at most the order of the group we have

(20) $2^{(p-1)} \leqq q^2 - 1 = W_p = \frac{1}{3}(1 + 2^p)$

a contradiction, completing the proof of sufficiency!

Thereby, completing the proof of the stated theorem!

Some Comment

The above proof rest on two possible innovations.

1) By extending the definition of 'order of the group' to elements which have no solution $g^k = 1$ but have solutions $g^k = \bar{g}^j$ The reasoning presented may not be knew and already documented somewhere and references are kindly requested. The reasoning is correct as $(a + \mathtt{i})^{(2k+1)} = (a - \mathtt{i}) \pmod{(a + \mathtt{i})}$ where $2k + 1$ is prime and k odd, thus the order of the group is 4k+2 as then the complex number sequence repeats.

2) The other innovation is the choice of the initial value of the iterator S_0 such that S_0 and S_1 do not repeat such that the equality (9) can be written, without this identity this proof is not possible.

3) One can construct a similar proof for $W_p = \frac{1}{3}(1 + 2^p)$ is prime if and only if $S'_p = S'_1 (mod\ W_p)$ where $S'_0 = \frac{-3}{2}$ and $S'_{n+1} = S'^2_n - 2$ and using $S'_{p-1} = -S'_0 (mod\ W_p)$. This alternate test has one more cycle than the the main test proven above. Furthermore, the initial S'_0 already use $2^{(p-1)}$ bits, so the lengthy FFT multiplication algorithm has to be used compared to the quick squaring of small integers for the first view cycles of S_n; overall when testing many numbers time saving is substantial.

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