

# Prime Numbers Arising from Quadratic Polynomials

Avineet Pannu

September 17, 2012

## Abstract

For  $f(1), f(2), \dots, f(n)$ , define  $\mathcal{S}(a, b, n)$  to be the smallest possible integer  $m$ , such that  $f(1), f(2), \dots, f(n)$  are all distinct  $(\text{mod } m)$ . Zhi-Wei Sun claims in his paper *A Simple Way to Generate All Primes* that he is able to generate exactly all primes using the quadratic  $f(t) = t(t - 1)$  and modulo arithmetic defined above. We used the function  $\mathcal{S}(a, b, n)$  and defined it using the coefficients of a quadratic in the form of  $f(t) = t(at + b)$  and  $n$  just being the term in the sequence. Continuing off of Zhi-Wei Sun's research which looked at  $\mathcal{S}(1, -1, n)$ , we explore the general case where  $b$  is left as a constant,  $\mathcal{S}(1, b, n)$ . Depending on the two different cases where  $b$  is either even or odd, we see that  $\mathcal{S}(1, b, n)$  is a combination of  $2p, 2^h$ , and  $p$ . After that, we show the results of two specific cases,  $\mathcal{S}(2, 1, n)$  and  $\mathcal{S}(3, 1, n)$ . Interestingly  $\mathcal{S}(2, 1, n)$  results in  $2^h$  for  $h$  such that  $n \leq 2^h$  and  $\mathcal{S}(3, 1, n)$  in  $3^h$  for  $h$  such that  $n \leq 3^h$ .

## 1 Introduction

For a very long time, mathematicians have been trying to find a polynomial that only outputs prime numbers. They have found formulas that at first give prime values, but they eventually fail. For example,  $p(n) = n^2 - n + 41$ . The first few terms are:  $n = 1$  then  $p(n) = 41$ ,  $n = 2$  then  $p(n) = 43$ ,  $n = 3$  then  $p(n) = 47$ ,  $n = 4$  then  $p(n) = 53$ ,  $n = 5$  then  $p(n) = 61$ ,  $n = 6$  then  $p(n) = 71$ ,  $n = 7$  then  $p(n) = 83$ . However when  $n = 41$ ,  $p(n) = 1681$ , which is  $41^2$ , therefore it is not prime. Thus at  $n = 41$ ,  $p(n)$  does not work.

Recently, Zhi-Wei Sun came up with a new idea that uses a function  $f(t) = t(t-1)$  and modulo arithmetic. Specifically, for a fixed integer,  $n > 1$  let  $m$  be the smallest integer such that  $f(1), f(2), \dots, f(n)$  are distinct modulo  $m$ . He claimed that the numbers in which arise this way are always prime. Therefore it is believed that this simple function has a value set of exactly all prime numbers.

Using the same method he explains in his paper *A Simple Way to Generate All Primes*, I used polynomials in the form of  $f(t) = at^2 + bt + c$ . However, since  $f(t_1) \equiv f(t_2) \pmod{m}$  iff  $f(t_1) - c \equiv f(t_2) - c \pmod{m}$ , we can instead just say  $f(t) = at^2 + bt = t(at + b)$ . Using this I began to find the first  $m$ , that would give me a pairwise incongruent answer when it is  $f(t) \pmod{m}$ . I called this function  $\mathcal{S}(a,b,n)$  or an abbreviated  $\mathcal{S}(n)$ ; also more commonly referred to as  $m$ . In Sun's case his function was  $\mathcal{S}(1,-1,n)$ . In the general case I looked at, I kept  $b$  as a variable to investigate how the final answer was different as the value of  $b$  changed. This function looked like  $\mathcal{S}(1,b,n)$ . The other two specific cases I looked at were  $\mathcal{S}(2,1,n)$  and  $\mathcal{S}(3,1,n)$ .

## 2 Proofs for the general case of $f(t) = t(t + b)$

**Theorem 1.** *Suppose  $n > 1$  is a fixed integer and  $m$  will denote an integer such that  $f(1), f(2), \dots, f(n)$  have distinct remainders  $\pmod{m}$ , then*

- (i)  $m \geq 2n + b$
- (ii)  $m$  is a prime or power of 2 when  $b$  is odd

*Proof of Theorem 1 (i).*

First do the case where  $m - b$  is even:

$$\text{Let } x = \frac{m-b}{2} + 1 \text{ and } y = \frac{m-b}{2} - 1.$$

Then using the function  $f(t) = t(t + b)$ ,  $f(x) - f(y) = x(x + b) - y(y + b) =$

$$\left(\frac{m-b}{2} + 1\right)\left(\frac{m-b}{2} + 1 + b\right) - \left(\frac{m-b}{2} - 1\right)\left(\frac{m-b}{2} - 1 + b\right).$$

This simplifies to

$$2(m-b) + 2b = 2m \equiv 0 \pmod{2m}.$$

Hence  $f(x) \equiv f(y) \pmod{m}$ . We call this a collision. Because  $f(1), f(2), \dots, f(n)$  are distinct  $\pmod{m}$ , we must have  $x > n$ .

$$x = \frac{m-b}{2} + 1 > n \text{ we easily see that } m \geq 2n + b.$$

Now if  $m-b$  is odd:

$$\text{let } x = \frac{m-b+1}{2} \text{ and } y = \frac{m-b-1}{2}.$$

Then using the collision between  $x$  and  $y$  we obtain  $f(x) - f(y) =$

$$\left(\frac{m-b+1}{2}\right)\left(\frac{m-b+1}{2} + b\right) - \left(\frac{m-b-1}{2}\right)\left(\frac{m-b-1}{2} + b\right),$$

which simplifies to

$$\frac{1}{4}(2m - 2b + 2b + 2m - 2b + 2b) = m$$

Again  $f(x) \equiv f(y) \pmod{m}$ . Therefore using the same previous reasoning  $x > n$

$$x = \frac{m-b+1}{2} > n, \text{ which leads to } m \geq 2n + b. \quad \square$$

**Lemma 2.** *When  $b$  is odd, we cannot have  $m = 2p$  for  $p$  an odd prime.*

*Proof of Lemma 2.*

So by contradiction, suppose  $m = 2p$ .

$$\text{Let } x = \frac{p-b}{2} + 1 \text{ and } y = \frac{p-b}{2} - 1.$$

Then using previous methods of collision between  $x$  and  $y$  we obtain

$$\left(\frac{p-b}{2} + 1\right)\left(\frac{p-b}{2} + 1 + b\right) - \left(\frac{p-b}{2} - 1\right)\left(\frac{p-b}{2} - 1 + b\right),$$

which simplifies to

$$2(p-b) + 2b = 2p \equiv 0 \pmod{2p}.$$

Thus  $x > n$  which leads to

$$\frac{p-b}{2} + 1 > n \text{ leading to } 2n + b \leq p = \frac{m}{2}$$

which is impossible since we already established that  $m$  itself has to be greater than  $2n + b$ . Therefore it is not possible that  $m/2$  is also greater than  $2n + b$ . Thus  $m$  cannot be  $2p$ .  $\square$

**Lemma 3.** *For any  $b$  we cannot have  $m$  divisible by  $p^2$  where  $p$  is an odd prime.*

*Proof of Lemma 3.*

By contradiction, assume  $p^2 \mid m$

For the case where  $b$  is odd,

$$\text{let } x = y + pq \text{ and } y = \frac{p-b}{2}.$$

Then using the same collision as before between  $x$  and  $y$  we obtain

$$\left(\frac{p-b}{2} + pq\right)\left(\frac{p-b}{2} + pq + b\right) - \left(\frac{p-b}{2}\right)\left(\frac{p-b}{2} + b\right),$$

which simplifies to

$$pq(pq + p) \equiv 0 \pmod{pq}. \text{ Hence } f(x) \equiv f(y) \pmod{m}.$$

Now looking at the case where  $b$  is even, let  $x = y + pq$  and  $y = \frac{2p-b}{2}$ . Then using the same collision as before between  $x$  and  $y$  we obtain

$$\left(\frac{2p-b}{2} + pq\right)\left(\frac{2p-b}{2} + pq + b\right) - \left(\frac{2p-b}{2}\right)\left(\frac{2p-b}{2} + b\right),$$

which simplifies to

$$pq(pq + 2p) \equiv 0 \pmod{pq}.$$

Since we have the same collision as before we can say that  $x > n$  which once again gives us a contradiction to the property of  $x$  and  $m$ .  $\square$

*Proof of theorem 1 (ii).*

We know that  $m$  is a number such that  $f(1), f(2), \dots, f(n)$  are distinct (mod  $m$ ). We know  $m \neq 2 * \text{odd}$  and  $m \nmid p^2$ . We want to show that  $m$  is a prime or a power of two when  $b$  is off. So assume That it is neither of those and therefore  $m = pq$  for  $p$  is an odd prime and  $p \nmid q$

$$\text{Let } x = y + p \text{ and } y = \frac{2}{\gcd(2, q)} - \frac{b + p}{2}.$$

In the case of  $2 \mid q$

$$\begin{aligned} x &= \frac{q}{2} - \frac{b}{2} + \frac{p}{2} < \frac{q}{2} + \frac{p}{2} \\ &= \frac{m}{2p} + \frac{m}{2q} \\ &= \frac{m}{2} \left( \frac{1}{p} + \frac{1}{q} \right). \end{aligned}$$

Now take the case that maximizes  $x$  to find the upper bound on  $x$ . Since  $p \nmid q$  and  $q > 2$ , the values of  $p$  and  $q$  that would maximize  $x$  are  $p=3$  and  $q=4$  which gives us

$$x \leq \frac{m}{2} \left( \frac{1}{3} + \frac{1}{4} \right). \text{ Therefore } x \leq \frac{7}{24}m.$$

Now taking the case where  $2 \nmid q$ :

$$\begin{aligned} x &= q - \frac{b}{2} + \frac{p}{2} < q + \frac{p}{2} \\ &= \frac{m}{p} + \frac{m}{2q} \\ &= m \left( \frac{1}{p} + \frac{1}{2q} \right). \end{aligned}$$

Now to find the upper bound on  $x$  we must maximize  $p$  and  $q$  using the same reasoning as before. But now  $q$  can not be even so the maximizing values are  $p=5$  and  $q=3$  which gives us

$$x \leq m \left( \frac{1}{5} + \frac{1}{6} \right). \text{ Therefore } x \leq \frac{11}{30}m.$$

In both cases they once again violate the properties of  $m$  and  $x$  and thus we have a contradiction. Therefore  $m$  must be a prime of a power of two if  $b$  is odd.  $\square$

Theorem 1 shows that the only possibilities for  $m$  are primes and powers of two. We are now going to show that if  $b$  is even then it can also be twice a prime. Taking all of these options, we are now going to show that if  $m \geq 2n + b$  then one of these options must be the answer to  $\mathcal{S}(n)$ .

**Theorem 4.** *If  $m$  is a prime, double prime, or power of two then  $f(x) \not\equiv f(y) \pmod{m}$  for any  $1 \leq y < x \leq n$*

*Proof of Theorem 4.*

case 1:  $m = 2^a$  and  $b$  is odd

First assume  $1 \leq y < x \leq n$  and note  $f(x)-f(y) = (x-y)(x+y+b)$ . We can easily attain  $1 \leq x - y < n \leq m = 2^a$ . Using the fact that  $b$  is odd then we know that  $x-y$  and  $x+y+b$  have opposite parity so one will be odd and one will be even. However we know that  $x - y$  is less than  $2^a$  therefore  $2^a \nmid x - y$ . We also need  $x + y + b < 2x + b < 2n + b < n = 2^a$ , which leads to  $2 \nmid x + y + b$ . Thus,  $2^a$  can not divide the product therefore  $f(x) \not\equiv f(y) \pmod{2^a}$  therefore  $n$  has a distinct remainder.

case 2:  $m = p$

Once again assume  $1 \leq y < x \leq n$  which can easily become  $1 \leq x - y < n \leq m = p$ . Taking the inequality we know that  $p$  can not divide  $x - y$  because it is too small. Therefore  $p$  must divide  $x + y + b$ . However assuming that  $x$  and  $y$  are not the same and that  $y$  is smaller than  $x$  we get  $x + y + b < 2x + b \leq 2n + b \leq m = p$ . Thus  $p$  cannot divide  $x+y+b$  and therefore  $f(x) \not\equiv f(y) \pmod{p}$  therefore  $n$  has a distinct remainder.

case 3:  $m = 2p$  and  $b$  is even

In the final case we again have  $x - y < \frac{m-b}{2} < p$  and  $x + y + b < 2n + b < m$ . Then for  $m$  to divide  $(x - y)(x + y + b)$ ,  $2$  and  $p$  must divide the product. However since  $x - y$  is smaller than  $p$ , it cannot be divisible by  $p$  therefore  $p$  must divide  $x + y + b$ . Since  $b$  is even we know that either  $x - y$  and  $x + y + b$  are both even or odd. However since  $2$  must divide one they are both even. Since  $p \mid x + y + b$  then  $x + y + b > p$ . Thus  $2p \mid x + y + b$ , therefore  $m < x + y + b < 2n + b$ . However since  $2p = m$ ,  $p$  cannot be greater than  $m$  thus  $p \nmid x + y + b$ . Therefore  $f(x) \not\equiv f(y) \pmod{2p}$  therefore  $n$  has a distinct remainder.  $\square$

For the general case the final conclusions that I was able to draw were

$$\mathcal{S}(1, b, n) = \begin{cases} 2^a \text{ or } p & \text{for } b \text{ odd} \\ 2p \text{ or } p & \text{for } b \text{ even.} \end{cases}$$

### 3 Proof for the specific case of $f(t) = t(2t + 1)$

Now take the case  $f(t) = t(2t + 1)$  which says we are looking for  $\mathcal{S}(2,1,n)$ .

**Theorem 5.**  $\mathcal{S}(n) = 2^h$  is the answer for the minimum  $h$  such that  $n \leq 2^h$ .

*Proof of Theorem 5.*

Proposition 1:

Note that  $f(x) \equiv f(y) \pmod{m}$  if and only if  $(x - y)(2(x + y) + 1) \equiv 0 \pmod{m}$ . Fix  $h$  such that  $2^h \geq n$ . Then  $f(1), \dots, f(n)$  are distinct modulo  $2^h$  and assume  $1 \leq y < x \leq n \leq m = 2^h$ .

Now taking the previous note into consideration,  $f(x) \equiv f(y) \pmod{2^h}$  if and only if  $(x - y)(2(x + y) + 1) \equiv 0 \pmod{2^h}$  but  $2(x + y) + 1$  is odd so it is not divisible by any multiple of 2. Thus this is only possible if  $x - y \equiv 0 \pmod{2^h}$ . However using the previous inequality,  $x - y$  is smaller than  $2^h$ , thus  $f(x) \not\equiv f(y)$ . Therefore  $n$  has a distinct remainder.  $\square$

Proposition 2: We try to show that  $m$  is even assuming  $2^{h-1} < n \leq \mathcal{S}(n) \leq 2^h$

Assume  $\mathcal{S}(n)$  is even and  $m \neq 2q$ . By contradiction let  $m = \mathcal{S}(n)$  be odd. Since  $m$  is odd,  $z = \frac{m-1}{2}$  is an integer.

$$\text{Let } x = \frac{z+1}{2} \text{ and } y = \frac{z-1}{2} \text{ if } z \text{ is odd.}$$

$$\text{Let } x = \frac{z+2}{2} \text{ and } y = \frac{z-2}{2} \text{ if } z \text{ is even.}$$

So then  $x - y = 1$  or  $2$  and  $2(x + y) + 1 = m$ . And  $f(x) \equiv f(y) \pmod{m}$ , therefore  $x > n$ . But then we have  $n < x = \frac{\frac{m-1}{2} + \epsilon}{2}$  for  $\epsilon = 1$  or  $2 \leq \frac{\frac{m-1}{2} + \frac{m+1}{2}}{2} = \frac{m}{2} < \frac{2^h}{2} = 2^{h-1} < n$  which gives us a contradiction to our original inequality. Therefore  $m$  cannot be odd.

Proposition 3:

Now suppose  $m = 2^t p$  for  $p$  odd and  $t \geq 1$ . Assume  $2^h - 1 < n \leq m < 2^h$

and  $f(1), f(2), \dots, f(n)$  are all distinct  $(\text{mod } m)$ . We now work towards a contradiction.

For  $p \equiv 1 \pmod{4}$  and  $t = 1$ , set  $k = 1$ . For  $p \equiv 1 \pmod{4}$  and  $t \geq 2$ , set  $k = 1 = 2^t$ . For  $p \equiv 3 \pmod{4}$ , set  $k = 3$  if  $t = 1$ . Otherwise set  $k = 3 + p^t$ .

Finally, let  $x_0 = \frac{kp-1}{4} + 2^{t-1}$  and  $y_0 = \frac{kp-1}{4} - 2^{t-1}$ . By choice of  $k$ ,  $x_0$  and  $y_0$  are both integers.

To show  $y > 0$  we fix  $p = 5$  and  $t = 1$ .

For  $t = 1$   $y = \frac{kp-1}{4} - 2^{1-1} = \frac{kp-1}{4} - 1$ .

Then  $p \equiv 1 \pmod{4}$  meaning that  $p$  must be greater than 5 which gives us  $\frac{kp-1}{4} - 1 > 0$ , continuing on  $p \equiv 3 \pmod{4}$ , which leads to  $kp \geq 9$ . Finally this shows that  $\frac{kp-1}{4} - 1 > 0$ .

Now show  $f(x) \equiv f(y) \pmod{m}$ , where  $m = 2^t p$   
 $x - y = 2^t, x + y = \frac{kp-1}{2}$  this leads to  $2(x + y) + 1 = kp$ . Therefore  $(x - y)(2(x + y) + 1) \equiv 0 \pmod{2^t p}$ . Thus we have the same collision and so we know that  $m$  cannot be just any even number.

Finally to show  $x < m/2$

$$x = \frac{kp-1}{4} - 2^{t-1} = \frac{k \frac{m}{2^t} - 1}{4} + \frac{m}{2p} = \frac{m}{2} \left( \frac{k}{2^{t+1}} + \frac{1}{p} \right) - \frac{1}{4}.$$

So we need

$$\frac{k}{2^{t+1}} + \frac{1}{p} \leq 1.$$

We then fix  $t = 1$  and  $p = 3$ .

When  $p \equiv 3 \pmod{4}$ , we get  $\frac{k}{2^{t+1}} + \frac{1}{p} \leq \frac{1}{4} + \frac{1}{5} < 1$ .

The next case is when  $p \equiv 3 \pmod{4}$ , which gives us  $\frac{k}{2^{t+1}} + \frac{1}{p} = \frac{3}{4} + \frac{1}{p} \leq \frac{3}{4} + \frac{1}{7} < 1$ .

However if  $t \geq 2$  we still have to satisfy the  $\frac{k}{2^{t+1}} + \frac{1}{p} \leq 1$ .

When  $p \equiv 1 \pmod{4}$  it results in,

$$\frac{k}{2^{t+1}} + \frac{1}{p} = \frac{1+2^t}{2^{t+1}} + \frac{1}{p} = \frac{1}{2^{t+1}} + \frac{1}{2} + \frac{1}{p} \geq \frac{1}{8} + \frac{1}{2} + \frac{1}{5} = \frac{33}{40} < 1$$

Therefore the condition is satisfied. When  $p \equiv 3 \pmod{4}$ ,

$$\frac{k}{2^{t+1}} + \frac{1}{p} = \frac{3+2^t}{2^{t+1}} + \frac{1}{p} = \frac{3}{2^{t+1}} + \frac{1}{2} + \frac{1}{p} \geq \frac{1}{8} + \frac{1}{2} + \frac{1}{5} = \frac{33}{40} < 1$$

The final conclusions for this function state that  $\mathcal{S}(2,1,n) = 2^h$  for  $h$  such that  $n \leq 2^h$ .



## 4 Proof for the specific case of $f(t) = t(3t + 1)$

Taking the case  $f(t) = t(3t + 1)$  is now saying we are looking for  $\mathcal{S}(3,1,n)$ .

**Theorem 6.**  $\mathcal{S}(n) = 3^h$  for  $h$  min such that  $n \leq 3^h$ , when  $n \geq 9$ .

*Proof of Theorem 6.*

Let  $h$  be such that  $3^h \geq n$ . Then  $f(1), f(2), \dots, f(n)$  are distinct  $(\text{mod } 3^h)$

Suppose  $f(x) \equiv f(y) \pmod{3^h}$  for  $1 \leq y < x \leq n < 3^h$ . Then  $(x-y)(3(x+y)+1)$  is divisible by  $3^h$ . But  $3 \nmid 3(x+y)+1$  since it is not a multiple of three, therefore 3 must divide  $x-y$ . So  $x \geq y+3^h$ . Which leads to a contradiction since  $x$  is already smaller than  $3^h$ .

Proposition 1:  $\mathcal{S}(n)$  must be divisible by 3.

On the contrary, suppose  $m = \mathcal{S}(n)$  and  $3 \nmid m$  and that  $3^{h-1} < n \leq m < 3^h$ , and  $f(1), \dots, f(n)$  are distinct modulo  $3^h$ .

$$\text{Let } z_0 = \begin{cases} \frac{m-1}{3} & \text{when } m \equiv 1(3) \\ \frac{2m-1}{3} & \text{when } m \equiv 2(3). \end{cases}$$

$$\text{Let } x_0 = \frac{z_0 + \epsilon}{2} \text{ and } y_0 = \frac{z_0 - \epsilon}{2}$$

Where  $\epsilon$  is 1 when  $z_0$  is odd and 2 when it is even.

$$\text{Then } (x-y) = \epsilon \text{ and } 3(x+y)+1 = 3z_0+1 = \begin{cases} m & m \equiv 1 \pmod{3} \\ 2m & m \equiv 2 \pmod{3}. \end{cases}$$

By definition of  $m$ , this implies  $x > n$ . So  $n < x_0 = \frac{z_0 + \epsilon}{2} = \frac{lm-1}{3} + \epsilon = \frac{lm}{6} - \frac{1}{6} + \frac{\epsilon}{2} < \frac{lm}{6} \leq m3 < 3^{h-1}$  where  $l = 1, 2$ . However  $3^{h-1} < n$  therefore we have a contradiction, thus  $3 \mid m$ .

Proposition 2:

So write  $m = 3^s p$  for  $p > 1$  and  $3 \nmid p, s \geq 1$ . As always, assume  $3^{h-1} < n \leq m < 3^h$  where  $h \geq 2$ , and  $f(1), f(2), \dots, f(n)$  are distinct modulo  $m$ .

Choose  $l$  by

$$l = \begin{cases} 4 + 6k & p \equiv 1 \pmod{6} \\ 2 + 6k & p \equiv 2 \pmod{6} \\ 1 + 6k & p \equiv 4 \pmod{6} \\ 2 + 6k & p \equiv 5 \pmod{6} \end{cases}$$

for  $k$  to be determined later. Now let

$$x_0 = \frac{lp - 1 + 3^{s+1}}{6} \text{ and } y_0 = \frac{lp - 1 - 3^{s+1}}{6}.$$

Since  $lp = 4 \pmod{6}$  and  $l \pm 3^{s+1} \equiv 3 \pmod{6}$  we see that  $lp - 1 \pm 3^{s+1}$  are divisible by 6. Therefore  $x_0$  and  $y_0$  are integers. Then using the knowledge, we can say that  $x_0 - y_0 = 3^s$  and  $x_0 + y_0 = \frac{lp-1}{3}$ . Therefore  $3(x_0 + y_0) + 1 = lp \equiv 0 \pmod{p}$  thus  $f(x_0) \equiv f(y_0) \pmod{m}$ .

Now when  $y_0 > 0$

$$y_0 = \frac{lp - 1 - 3^{s+1}}{6},$$

so  $y_0 > 0$  iff  $lp - 1 > 3^{s+1}$ , where  $l$  is to be chosen later. Therefore we get  $lp > 3^{s+1} + 1$

We need  $x_0 < m/3$

$$= \frac{lp - 1 + 3^{s+1}}{6} < \frac{m}{3}$$

This is only true iff  $lp - 1 + 3^{s+1} < 2m$  which can be written as,

$$\frac{lm}{3^s} - 1 + \frac{3m}{p} < 2m \text{ which simplifies to } m \left( \frac{l}{3^s} + \frac{3}{p} - 2 \right) < 1.$$

We will now choose  $l$  such that  $\frac{l}{3^s} + \frac{3}{p} - 2 \leq 0$ , that is  $lp \leq 3^s(2p - 3)$ . Now, if  $lp$  is so chose then  $f(x) \equiv f(y)$ , then  $x_0 > n$ . But  $x_0 < m/3 < 3^h/3 = 3^{h-1} < n$ . Therefore we have a contradiction. Our proof is complete once the conditions on  $lp$  are met. We need  $lp > 3^{s+1} + 1$  and  $lp \leq 3^s(2p - 3)$ .

We need  $lp > 3^{s+1} + 1$  and  $lp \leq 3^s(2p - 3)$ . That is  $l > \frac{3^{s+1}+1}{p}$  and  $l \leq 3^s(2 - \frac{3}{p})$ .

Suffice (to pick  $l = \epsilon + 6k$ ) to have  $\frac{3^{s+1}}{p} + 6 < 3^s(2 - \frac{3}{p})$ . For then we can pick  $k$  to have  $\frac{3^{s+1}+1}{p} < l = \epsilon + 6k < 3^s(2 - \frac{3}{p})$ . That is  $3^{s+1} + 6p < 3^s(2p - 3)$ , which is  $2 * 3 + 1 < (2 * 3^s - 6)p$ . And from this point just working out the algebra, we obtain  $\frac{2*3^{s+1}+1}{2*3^s-6} < p$ . Then we can now begin to break it all down and get

$$\frac{2 * 3 * 3^s - 18 + 18 + 1}{2 * 3^s - 6} = 3 + \frac{19}{2 * 3 - 6} < p$$

Now if  $s \geq 2$ , the previous statement is  $\leq 3 + 19/12 < 5$ . Therefore everything until now worked for  $p \geq 5$  and  $s \geq 1$ .

Now we do the case where  $s = 1$  and  $m = 3p$  where  $3 \nmid p$ .

We assume  $e^{h-1} < n \leq m < 3^h$  and that  $f(1), f(2), \dots, f(n)$  are distinct module  $m$ . We can check the small cases by hand, and so may assume  $p > 10$  and  $m > 24$ . Choose  $r = 1, 2$  or  $4$  so that  $rp \equiv 4 \pmod{6}$ . (So if

$p \equiv 1$  then  $r = 4$ , if  $p \equiv 2$  then  $r = 2$  etc.) Set  $x = \frac{rp+8}{6}$  and  $y = rp - 106$ . By the choice of  $r$ ,  $x$  and  $y$  are both integers, and because  $p > 10$ , both are positive integers.

Now  $x - y = 3$  and  $3(x + y) + 1 = rp$ . Thus  $f(x) \equiv f(y) \pmod{m}$ , and so  $n < x$ . We have  $x = \frac{rp+8}{6} = \frac{rm}{18} + \frac{8}{6} \leq \frac{4m}{18} + \frac{8}{6}$ . And because  $m > 24$  is it easy to see that this last value is greater than  $m/3$ . But then  $3^{h-2} < n < x < m/3 < 3^{h-1}/3 = 3^{h-1}$ . Therefore we have a contradiction. From which we can now say that  $m$  is not just a multiple of 3.  $\square$

The final results of the last case of  $\mathcal{S}(3,1,n) = 3^h$  for  $h$  such that  $n \leq 3^h$ .

## 5 References

Sun, Z. (2012, March 6). A Simple Way to Generate all Prime. Retrieved March 18, 2012, from <http://math.nju.edu.cn/zwsun>

## 6 Acknowledgements

Jim Sauerberg  
 Saint Mary's College of California  
 Summer Research Program 2012