CONSECUTIVE COMPOSITE VALUES OF A QUADRATIC POLYNOMIAL

Don Redmond

Southern Illinois University

Let a, b, and c be integers such that $b^2 - 4ac$ is not a perfect square. We are interested in finding sequences of integers n such that $an^2 + bn + c$ is composite. Of course, if $b^2 - 4ac$ is a perfect square, then $an^2 + bn + c$ is always composite. We follow along the lines of Garrison in [1].

Let $\mathcal{P} = \{p_t\}_{t=0}^{+\infty}$ be the sequence of primes such that $p_0 = 2$, $p_t < p_{t+1}$ and for all $p \in \mathcal{P}$ $((b^2 - 4ac)/p) = +1$, where (here and below) (m/p) denotes the Legendre symbol. Then $\mathcal{P}$ contains the prime divisors of all the $an^2 + bn + c$. Let

$$P(t) = \prod_{k=0}^{t} p_k$$

and let

$$C(t) = \{n : (an^2 + bn + c, P(t)) > 1\} .$$

For $i = 1$ and 2 let a_{ik} be the solutions to $an^2 + bn + c \equiv 0 \pmod{p_k}$ and let

$$S(t) = \{x : x \not\equiv 1 \pmod 2 \ \text{ and } \ x \not\equiv a_{ik} \pmod{p_n}, h = 1, \ldots, t\} .$$

Then we see that $(an^2+bn+c, P(t)) = 1$ if and only if $n \in S(t)$. Finally, by the Chinese Remainder Theorem, any complete residue system modulo $P(t)$ contains

$$Q(t) = \prod_{k=1}^{t} (p_k - 2)$$

solutions of $S(t)$.

Lemma 1. Let m be a fixed squarefree integer. Then there exists a constant A such that, as $x \to +\infty$,

$$\sum_{\substack{p \leq x \\ (\frac{m}{p})=+1}} \frac{1}{p} = \frac{1}{2}\log\log x + A + O\left(\frac{1}{\log x}\right) .$$

Proof. Now m is a quadratic residue of exactly those primes in certain residue classes modulo $4m$, in fact in exactly half of the $\phi(4m)$ residue classes modulo $4m$ that contain an infinitude of primes. Say these residue classes are

$$l_1, \ldots, l_{\phi(4m)/2} .$$

Then

$$\sum_{\substack{p \leq x \\ (\frac{m}{p})=+1}} \frac{1}{p} = \sum_{j=1}^{\phi(4m)/2} \sum_{\substack{p \leq x \\ p \equiv l_j \pmod{4m}}} \frac{1}{p} .$$

By a result of Mertens [2, p. 62], we have, as $x \to +\infty$,

$$\sum_{\substack{p \leq x \\ p \equiv l_j \pmod{4m}}} \frac{1}{p} = \frac{1}{\phi(4m)}\log\log x + \frac{c(m,l_j)}{\phi(4m)} + O\left(\frac{1}{\log x}\right) ,$$

where $c(m, l_j)$ is a certain constant. Thus we may take

$$A = \frac{1}{\phi(4m)} \sum_{j=1}^{\phi(4m)/2} c(m, l_j) \ ,$$

which proves the lemma.

One can show, from Mertens' paper that

$$A = \frac{1}{2}\left\{\gamma - H - \sum_{p|4m} \frac{1}{p}\right\} + \sum_{p} \frac{(m/p)}{p} \ ,$$

where γ is Euler's constant and $H = 0.31571845205$.

Lemma 2. There is a constant λ such that, as $t \to +\infty$,

$$\prod_{k=1}^{t} \frac{p_k}{p_k - 2} \sim \lambda \log p_t \ .$$

Proof. If $p \in \mathcal{P}$ and

$$s(p) = -\log\left(1 - \frac{2}{p}\right) - \frac{2}{p} = \sum_{k=2}^{+\infty} \frac{2^k}{kp^k} \ ,$$

then

$$2/p^2 < s(p) < (1/2)(2^2/p^2 + 2^3/p^3 + \cdots) = 2/p(p-2) \ .$$

Thus for $p \in \mathcal{P}$ we have that $s(p) > 0$. Also there exists a positive constant B such that

$$\sum_{k=1}^{+\infty} s(p_k) = B$$

and a function $\epsilon(t)$ such that $\lim_{t\to 0}\epsilon(t) = 0$ and

$$\sum_{k=1}^{t} s(p_k) = B - \epsilon(t) \ .$$

Thus

$$\sum_{k=1}^{t} \log \frac{p_k}{p_k - 2} = \sum_{k=1}^{t} \frac{2}{p_k} + B - \epsilon(t) \ .$$

If we let m denote the squarefree kernel of $|b^2 - 4ac|$, then we know that the elements of $\mathcal{P}$, except $p_0 = 2$, lie in $\phi(4m)/2$ residue classes modulo $4m$. Thus, by Lemma 1,

$$\sum_{k=1}^{t} \frac{2}{p_k} = \log\log p_t + 2A + O\left(\frac{1}{\log p_t}\right) \ ,$$

and so

$$\begin{aligned}\prod_{k=1}^{t} \frac{p_k}{p_k - 2} &= \exp\left(\sum_{k=1}^{t} \frac{2}{p_k} + B - \epsilon(t)\right) \\ &= (\log p_t)\exp\{2A + B - \epsilon(t) + O(1/\log p_t)\} \ .\end{aligned}$$

If we let $\lambda = \exp(2A + B)$, then the result follows and completes the proof.

Since the values of A and B depend on m we cannot, in general, give estimates of their values. In the two examples below we will compute the value of λ.

Note that a corollary of Lemma 2 is that

$$P(t)/Q(t) \sim 2\lambda \log p_t \ ,$$

as $t \to +\infty$.

We now state and prove our main result, which states that we can find arbitrarily long sequences of consecutive integers such that $an^2 + bn + c$ is composite.

Theorem. Let ϵ be a fixed real number such that $0 < \epsilon < 1$. Then for each sufficiently large $p_t \in \mathcal{P}$ there exists an integer X such that $X + h$ is not a solution of $S(t)$ for $h = 1, 2, \ldots, [(1-\epsilon)\lambda p_t]$ and $p_t \le X \le P(t) - p_t$.

Proof. Choose δ so that $0 < \delta < \min\left(\frac{1}{2}(1 - \sqrt{1-\epsilon}), \frac{3}{14}\right)$. Now choose $p_t \in \mathcal{P}$ large enough so that

$$i) \qquad (1 - 2\delta/3)\frac{x}{2\log x} \le \sum_l \pi(x, 4m, l) \le (1 + 2\delta/3)\frac{x}{2\log x} ,$$

for all $x > \delta p_t$, where (here and below) the sum over l denotes a sum over those residue classes modulo $4m$ that contains the primes in $\mathcal{P}$,

$$ii) \qquad (1 - 2\delta/3)2\lambda \log p_s < P(s)/Q(s) < (1 + 2\delta/3)2\lambda \log p_s$$

for all $p_s < \delta p_t$ and

$$iii) \qquad \log(\delta p_t) > (1 - 2\delta/3)\log p_t \ .$$

(Note that iii) implies that $p_t > \delta^{-3/2\delta}$.) Finally, let p_r be the least prime in $\mathcal{P}$ greater than p_t.

If y is a positive integer, let $N(y)$ be the number of solutions of $S(r)$ in $(y, y+(1-\epsilon)\lambda p_t]$.

Thus

$$\sum_{y=1}^{P(r)} N(y) = [(1-\epsilon)\lambda p_t]Q(r) \ ,$$

since each of the $Q(r)$ solutions in $S(r)$ is counted exactly $[(1-\epsilon)\lambda p_t]$ times on the left.

Thus, there exists a positive integer x such that $x \le P(r)$ and

$$\begin{aligned} N(x) &\le (1-\epsilon)\lambda p_t Q(r)/P(r) \\ &< \frac{(1-2\delta)^2 \lambda p_t}{(1-2\delta/3)2\lambda \log p_t} \\ &< (1-2\delta)p_t/(2\log p_t) \ , \end{aligned}$$

where we have used ii) and the condition that $\delta < (1-\sqrt{1-\epsilon})/2$. Also, by i), iii) and the condition that $\delta < \frac{3}{14}$, we see that the number of primes in $\mathcal{P}$ between p_r and p_t is

$$\begin{aligned} \sum_l \{\pi(p_t, 4m, l) - \pi(p_r, 4m, l)\} &> \frac{(1-2\delta/3)p_t}{2\log p_t} - \frac{(1+2\delta/3)\delta p_t}{2\log(\delta p_t)} \\ &> \frac{(1-2\delta/3)p_t}{2\log p_t} - \frac{(1+2\delta/3)\delta p_t}{(1-2\delta/3)2\log p_t} \\ &> (1-2\delta)p_t/(2\log p_t) \\ &> N(x) \ . \end{aligned}$$

Now let $x+h_1, \ldots, x+h_{N(x)}$ be the solution of $S(r)$ in the interval $(x, x+(1-\epsilon)\lambda p_t]$. By the Chinese Remainder Theorem there exists a positive integer X such that $X \le P(t)$, $X \equiv x \pmod{P(r)}$, $X \equiv a_k - h_{k-r} \pmod{p_k}$, for $k = r+1, \ldots, r+N(r)$, and $X \equiv 0 \pmod{p_k}$, for $k = r + N(x) + 1, \ldots, t$. This X satisfies the conditions of the theorem except possibly when X might be equal to $P(t)$. If this is the case we then use the positive integer X', where $X' \equiv X \equiv 0 \pmod{P(t-1)}$ and $X' \equiv 1 \pmod{p_t}$ with $P(t-1) \le x' \le P(t)$. This completes the proof of the theorem.

We now give two examples of the theorem. We will take $\epsilon = \frac{1}{2}$ in both examples. This forces a certain inequality on δ in the proof of the theorem, namely $\delta < .146446609$. This, in turn, forces $p_t > 3.6 \cdot 10^8$. Thus, our sequences of composites are long, but reasonably far out. If we choose ϵ close to 1, which would give us a short interval, we can lower the lower bound on p_t to around 50000.

Example 1. Let $a = 1$, $b = 0$, $c = 1$, that is, we take as our quadratic polynomial n^2+1. Here $b^2 - 4ac = -4$ and $m = 1$. Also $\mathcal{P}$ consists of those primes p such that $(-\frac{4}{p}) = +1$, that is, those primes for which -1 is a quadratic residue. As is well known, these are the primes of the form $4k+1$. In [2, p. 58] we find that $A = -.2867420562$ and Garrison shows in [1] that $.14059 < B < .14115$. Thus $.648 < \lambda < .649$. Thus, with $\epsilon = \frac{1}{2}$, if p is a prime of the form $4k+1$ that is sufficiently large, then the interval (p, P), where

$$P = \prod_{\substack{q \in P \\ q < p}} q \ ,$$

there is a sequence of consecutive integers, n, of length at least $.324p$ for which $n^2 + 1$ is composite.

Example 2. Here we take as our quadratic polynomial $n^2 - 2$. In this case $b^2 - 4ac = 8$ and $m = 2$. Now $(2/p) = +1$ if and only if $p \equiv \pm 1 \pmod 8$. As a special case of the result of Mertens [2, p. 62] we find that $A = -.6821954894$ and also we find, upon approximating the sum of the $s(p_k)$ that $.0697 < B < .0699$. Thus, in this case $.2739 < \lambda < .2740$. With the notation as in example 1 we see that if $p \equiv \pm 1 \pmod 8$ is sufficiently large, then the interval (p, P) contains a sequence of consecutive integers, n, of length at least $.137p$ for which $n^2 - 2$ is composite.

References

1. B. Garrison, "Consecutive Integers for which $n^2 + 1$ is Composite," *Pac. J. Math.*, 97 (1981), 93–96.
2. F. Mertens, "Ein Beitrag zur Analytischen Zahlentheorie," *J. Reine U. Angew. Math.*, 78 (1874), 46–62.