An Algorithm for $P(n^2 + c)$

Hans Oberschelp (joint work with Emma Mavis)

University of California, Davis

December 19, 2017

Rewording the Question

Given some prime p we want to find N such that if $n > N$, $P(n^2 + c) > p$.

In other words, we want to show that there are finitely many numbers of the form $n^2 + c$ with all primes in the prime factorization p or smaller.

In other words, we want to look at $n^2 + c = p_1^{b_1} \cdot ... \cdot p_j^{b_j}$ and show that $b_1, ..., b_j$ are all bounded.

Right off the bat...

Some primes may not divide $n^2 + c$ ever

$$p \mid n^2 + c$$

$$n^2 + c \equiv 0 \pmod{p}$$

$$n^2 \equiv -c \pmod{p}$$

$$\left(\frac{-c}{p}\right) = 1$$

Basic Idea

We pull out all the squares

$$n^2 + c = {p_1}^{d_1+2a_1} \cdot \ldots \cdot {p_k}^{d_k+2a_k}$$

where $d_i \in \{0, 1\}$

$$n^2 + c = D({p_1}^{a_1} \cdot \ldots \cdot {p_k}^{a_k})^2$$

where $D = {p_1}^{d_1} \cdot \ldots \cdot {p_k}^{d_k}$

And so we have 2^k possible D. Now we examine each case of D.

Pell Equation

Given some D, we let $y = {p_1}^{a_1} \cdot ... \cdot {p_k}^{a_k}$ and we let $x = n$

$$n^2 + c = D({p_1}^{a_1} \cdot ... \cdot {p_k}^{a_k})^2$$
$$x^2 + c = Dy^2$$
$$x^2 - Dy^2 = -c$$

Wow! A Pell Equation! I know how to solve those.

Eligible D Values for the Pell Equation

To find solutions to this Pell equation, we must look to how $-c$ factors in $\mathbb{Q}(\sqrt{D})$, the quadratic field generated by a specific D value

If $-c$ does factor, it must be of the form:

$$-c = (x + y\sqrt{D})(x - y\sqrt{D})$$

We now must turn to factoring ideals

Eligible D Values for the Pell Equation

3 possibilities for an ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, the ring of integers in the quadratic field:

$$(-c) = \mathfrak{p}\overline{\mathfrak{p}} \qquad \text{(split)} \qquad (1)$$

$$(-c) = \mathfrak{p}^2 \qquad \text{(ramified)} \qquad (2)$$

$$(-c) = \mathfrak{p} \qquad \text{(inert)} \qquad (3)$$

A solution to the Pell equation will only arise in the first situation, because that is when $-c$ factors into conjugates

In particular, a solution exists when $\mathfrak{p}$ is split and when $\mathfrak{p}$ is principal ideal, α

Then,

$$\alpha = (x + y\sqrt{D}), \quad {}^{*}N(\alpha) = \pm c$$

*$N(\alpha) = \alpha \cdot \overline{\alpha} = (x + y\sqrt{D})(x - y\sqrt{D}) = x^2 - Dy^2 = -c$

Eligible D Values for the Pell Equation

Solutions to our Pell equation are then found by multiplying powers of ϵ, the fundamental unit in $\mathbb{Q}(\sqrt{D})$, by α

- ϵ is found by taking a convergent of the continued fraction of $\sqrt{D}$

In order to be a solution though, $N(\alpha \cdot \epsilon^n) = -c$

Since $N(\epsilon)$ can be ± 1, we have 4 situations to consider:

i. $N(\alpha) = -c, \ N(\epsilon) = 1$
ii. $N(\alpha) = -c, \ N(\epsilon) = -1$
iii. $N(\alpha) = c, \ N(\epsilon) = -1$
iv. $N(\alpha) = c, \ N(\epsilon) = 1$

Recurrence Relation From the Pell Equation

Solutions to Pell equation follow recurrence pattern

- Generated by multiplying intitial solution, α, by powers of fundamental unit, ϵ

For each equation, we are able to find order 2 recurrence relation for just y solutions of the form:

$$y_{n+2} = ky_{n+1} - y_n$$

The coefficient k is always 2 times the rational component of ϵ (or ϵ^2), and coefficient of y_n is always -1

This sequence of y solutions (y_n) modulo any number is purely periodic because of this -1 coefficient (Engstrom)

Subcases for each D

So the idea is now to look at this sequence mod a bunch of numbers, and try to get some contradiction.

We want to find something like:

$$y = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot {p_3}^{a_3} \cdot ... \equiv k_{11},\ k_{12},\ k_{13},\ ... \pmod{m_1}$$
$$y = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot {p_3}^{a_3} \cdot ... \equiv k_{21},\ k_{22},\ k_{23},\ ... \pmod{m_2}$$
$$y = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot {p_3}^{a_3} \cdot ... \equiv k_{31},\ k_{32},\ k_{33},\ ... \pmod{m_3}$$
$$...$$

The problem is we usually can't generate a strong enough system to have no solutions. So we go deeper... We add even more subcases.

Subcases

To get extra information, we will look at subcases of which primes do and do not divide y.

For example if we have $y = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdot {p_3}^{a_3}$ for one case we say p_1 and p_2 divide y and p_3 does not.

So in this case $y = {p_1}^{a_1} \cdot {p_2}^{a_2}$ and also $y \equiv 0 \pmod{p_1 \cdot p_2}$

The nice thing about these subcases is that if we include few primes, we have a strong condition on the prime factorization of y, and if we include many primes we have a strong condition on the congruency to 0.

Example: $c = 3$, $p < 19$, $D = 7$, IN: 2, 7 OUT: 13

We assume 14 divides y.
We look at the period of y_s mod 14, and try to find primes that give y_s a period that is a multiple of the period mod 14.
This way the periods fit together, and we can use the "zeros" in the period mod 14 to easily see what y_s can be congruent to for these primes.

$2^a \cdot 7^b = 1 \pmod{13}$
$2^a \cdot 7^b = 14, 15 \pmod{29}$
$2^a \cdot 7^b = 14, 35, 78, 99 \pmod{113}$
$2^a \cdot 7^b = 14, 183 \pmod{197}$

Solutions:
$2^1 \cdot 7^1$
$2^{2339} \cdot 7^{2339}$

Example: $c = 3$, $p < 19$, $D = 7$, IN: 2, 7 OUT: 13

So how do we deal with the fact that $2^a \cdot 7^b$ has an actual solution? Simple! We just look at two new subcases, where y is divisible by $2 \cdot 7^2$, and where y is divisible by $2^2 \cdot 7$.

For y divisible by $2 \cdot 7^2$:

$$2^{a_1} \cdot 7^{b_2} \equiv 448,\ 925 \pmod{1373}$$
$$2^{a_1} \cdot 7^{b_2} \equiv 128,\ 333,\ 413,\ 791,\ 824,\ 1322,\ 1335,\ 1531,\ 1606,\ 1802,\ 1815,\ 2313,\ 2346,\ 2724,\ 2804,\ 3009 \pmod{3137}$$
$$2^{a_1} \cdot 7^{b_2} \equiv 361,\ 395,\ 734,\ 770,\ 771,\ 851,\ 1095,\ 1246,\ 1541,\ 1988,\ 2283,\ 2434,\ 2678,\ 2758,\ 2759,\ 2795,\ 3134, 3168 \pmod{3529}$$

has no solutions.

For y divisible by $2^2 \cdot 7$, it actually turns out that 4 never divides y. So we are done.

Showing the System Has No Solutions

$$p_1{}^{a_1} \cdot p_2{}^{a_2} \cdot p_3{}^{a_3} \cdot ... \equiv k_{11},\ k_{12},\ k_{13},\ ... \pmod{m_1}$$
$$p_1{}^{a_1} \cdot p_2{}^{a_2} \cdot p_3{}^{a_3} \cdot ... \equiv k_{21},\ k_{22},\ k_{23},\ ... \pmod{m_2}$$
$$p_1{}^{a_1} \cdot p_2{}^{a_2} \cdot p_3{}^{a_3} \cdot ... \equiv k_{31},\ k_{32},\ k_{33},\ ... \pmod{m_3}$$
$$...$$

Let r_i be a primitive root mod m_1.
Let h_{ij} be defined such that $r_i^{h_{ij}} \equiv p_j \text{ mod } (m_i)$.
Let ℓ_{ij} be defined such that $r_i^{\ell_{ij}} \equiv k_{ij} \text{ mod } (m_i)$.
Then:

$$h_{11} \cdot a_1 + h_{12} \cdot a_2 + h_{13} \cdot a_3 + ... \ \equiv \ell_{11},\ \ell_{12},\ \ell_{13},\ ... \pmod{\phi(m_1)}$$
$$h_{21} \cdot a_1 + h_{22} \cdot a_2 + h_{23} \cdot a_3 + ... \ \equiv \ell_{21},\ \ell_{22},\ \ell_{23},\ ... \pmod{\phi(m_2)}$$
$$h_{31} \cdot a_1 + h_{32} \cdot a_2 + h_{33} \cdot a_3 + ... \ \equiv \ell_{31},\ \ell_{32},\ \ell_{33},\ ... \pmod{\phi(m_3)}$$
$$...$$

Showing the System Has No Solutions

Now we just have to check for all possible combinations of ℓ.

$$\begin{aligned} h_{11} \cdot a_1 + h_{12} \cdot a_2 + h_{13} \cdot a_3 + \ldots &\equiv \ell_1 \pmod{\phi(m_1)} \\ h_{21} \cdot a_1 + h_{22} \cdot a_2 + h_{23} \cdot a_3 + \ldots &\equiv \ell_2 \pmod{\phi(m_2)} \\ h_{31} \cdot a_1 + h_{32} \cdot a_2 + h_{33} \cdot a_3 + \ldots &\equiv \ell_3 \pmod{\phi(m_3)} \\ &\ldots \end{aligned}$$

We can solve this first by converting each line to the same modulus:

Let $w := \operatorname{lcm}(\phi(m_1), \phi(m_2), \phi(m_3), \ldots)$
Let $w_i := \frac{w}{\phi(m_i)}$

$$\begin{aligned} w_1 \cdot (h_{11} \cdot a_1 + h_{12} \cdot a_2 + h_{13} \cdot a_3 + \ldots) &\equiv w_1 \cdot k_1 \pmod{w} \\ w_2 \cdot (h_{21} \cdot a_1 + h_{22} \cdot a_2 + h_{23} \cdot a_3 + \ldots) &\equiv w_2 \cdot k_2 \pmod{w} \\ w_3 \cdot (h_{31} \cdot a_1 + h_{32} \cdot a_2 + h_{33} \cdot a_3 + \ldots) &\equiv w_3 \cdot k_3 \pmod{w} \\ &\ldots \end{aligned}$$

Solutions!

All the solutions for $P(n^2+3) < 19$ are:

$1^2+3 = 1 \cdot (2)^2$

$0^2+3 = 3$

$3^2+3 = 3 \cdot (2)^2$

$12^2+3 = 3 \cdot (7)^2$

$45^2+3 = 3 \cdot (2 \cdot 13)^2$

$2^2+3 = 7$

$5^2+3 = 7 \cdot (2)^2$

$37^2+3 = 7 \cdot (2 \cdot 7)^2$

$7^2+3 = 13 \cdot (2)^2$

$9^2+3 = 21 \cdot (2)^2$

$6^2+3 = 39$

$306^2+3 = 39 \cdot (7^2)^2$

$19^2+3 = 91 \cdot (2)^2$

$124^2+3 = 91 \cdot (13)^2$

$33^2+3 = 273 \cdot (2)^2$

So when $n > 306$, $P(n^2+3) \geq 19$.

Solutions!

We also found all the solutions for $P(n^2+5) < 23$:
$2^2+5 = 1 \cdot (3)^2$
$0^2+5 = 5$
$20^2+5 = 5 \cdot (3^2)^2$
$10^2+5 = 105$
$830^2+5 = 105 \cdot (3^4)^2$
$3^2+5 = 14$
$11^2+5 = 14 \cdot (3)^2$
$101^2+5 = 14 \cdot (3^3)^2$
$25^2+5 = 70 \cdot (3)^2$
$1^2+5 = 6$
$7^2+5 = 6 \cdot (3)^2$
$17^2+5 = 6 \cdot (7)^2$
$5^2+5 = 30$
$115^2+5 = 30 \cdot (3 \cdot 7)^2$
So when $n > 830$, $P(n^2+5) \geq 23$.

Subleties of choosing moduli

There are 3 forces fighting against each other:

- We actually need to find useful moduli, which is easier if we relax the restriction that y has few congruences.
- We want to find as many moduli as possible, because the more we have to more likely the system has no solutions.
- As we increase the moduli and increase the congruences the difficulty of solving the system grows exponentially.

Improvements

It is possible that our algorithm would run faster if we allowed primes, q_i that were not multiples of the period of z, or at least had $\gcd(\text{period}(q_i), \text{period}(z)) > 1$, provided that they had very short periods. The idea is that adding a line to the system of linear congruences with few k's on the right hand side would be beneficial, even if it does not use any information from requiring y is divisible by z. Provided there are no solutions for y, it may be even possible to prove so without using any z divisibility information for any k. We tried to do this and were not able to. Of course if y does have solutions, it is impossible to go without information from z divisibility. We need that information to rule out actual solutions of y. It seems reasonable that using a combination of k, some with very short periods, and others with periods that are multiples of z, may lead to better results.

Our algorithm is written to only deal with prime values of c. Considering composite values would mean much more extensive algebraic number theory in that we would have to reevaluate the ideal factoring in the quadratic field.

Special Thanks

Thank you to Kevin McGown for hosting the REU at CSU Chico and inviting me to be a part of it.

Thank you to the National Science Foundation for funding the Chico REU. (NSF grant DMS-1559788)