CS 417
Algorithm to write a prime as a sum of squares

Enrique Treviño

March 10, 2024

1 Introduction

These notes are written to describe an algorithm, due to Rabin and Shallit [1], that can find for a prime $p \equiv 1 \mod 4$, two positive integers a, b such that $a^2 + b^2 = p$.

2 Preliminaries on Quadratic Residues

Let p be an odd prime number. We say that a is a *quadratic residue* modulo p if a is not a multiple of p and there exists an integer x such that $x^2 \equiv a \bmod p$. For example, modulo 7, the quadratic residues are 1,2, and 4, because $1^2 \equiv 1 \bmod 7, 2^2 \equiv 4 \bmod 7$, and $3^2 \equiv 2 \bmod 7$. We say that a is a *quadratic non-residue* modulo p if a is not a multiple of p and there does not exist an integer x such that $x^2 \equiv a \bmod p$. For example, modulo 7, the quadratic non-residues are 3, 4, and 6.

From this definition we can now define the Legendre symbol, $\left(\frac{a}{p}\right)$:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a, \\ 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p. \end{cases}$$

For example, $\left(\frac{14}{7}\right) = 0, \left(\frac{3}{7}\right) = -1, \left(\frac{11}{7}\right) = 1$.

From the definition of the Legendre symbol, it is easy to see that the Legendre symbol is periodic with period p (because it's defined modulo p). One can also see that $\left(\frac{1}{p}\right) = 1$ for any p since $1^2 \equiv 1 \bmod p$.

Here are other results involving the Legendre symbol:

Theorem 1. Let p be an odd prime. Then there are $(p-1)/2$ quadratic non-residues and mod$p$ and $(p-1)/2$ quadratic residues mod$p$ between 1 and $p-1$.

Proof. First note that $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2 \bmod p$ are all distinct modulo p. Indeed, if $i^2 \equiv j^2 \bmod p$, we have $i^2 - j^2 \equiv 0 \bmod p$, which implies $(i-j)(i+j) \equiv 0 \bmod p$. But because p is prime, that implies that $i \equiv -j \bmod p$ or $i \equiv j \bmod p$. Note that if $i, j \in \{1, 2, \ldots, (p-1)/2\}$, then $i \not\equiv -j \bmod p$, so if $i^2 \equiv j^2$, then $i \equiv j \bmod p$. Therefore, each value is distinct. That means we have at least $(p-1)/2$ quadratic residues mod$p$.

On the other hand, note that $i^2 \equiv (p-i)^2 \bmod p$, so $\left(\frac{p-1}{2}+1\right)^2 \equiv \left(p - \left(\frac{p-1}{2}\right)\right)^2 \bmod p, \ldots, (p-1)^2 \equiv 1^2 \bmod p$. Therefore, there can't be any other quadratic residues. That means there are $(p-1)/2$ quadratic residues modulo p and the rest are quadratic non-residues. The rest is $(p-1)/2$, so the proof is complete. □

The above result is nice, but the result we will need for our algorithm is the following:

Theorem 2 (Euler's Criterion)**.** Let p be an odd prime. Then

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Proof. If $a \equiv 0 \bmod p$, then $\left(\frac{a}{p}\right) = 0$ and $a^{(p-1)/2} \equiv 0 \bmod p$, so the theorem is true in that case.

We may therefore assume that $a \not\equiv 0 \bmod p$.

Suppose that $\left(\frac{a}{p}\right) = 1$. Then, there exists x such that $x^2 \equiv 1 \bmod p$. Note that $x \not\equiv 0 \bmod p$ because $a \not\equiv 0 \bmod p$.

Therefore

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p.$$

The last equality follows from Fermat's Little Theorem.[1]

We have shown that $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$ when $\left(\frac{a}{p}\right) = 1$. Note that $\left(\frac{a}{p}\right) = 1$ occurs for $(p-1)/2$ values. Therefore, we have at least $\frac{p-1}{2}$ roots to the polynomial $x^{\frac{p-1}{2}} - 1 \bmod p$. But, a polynomial modulo p of degree n can have at most n roots (this is known as Lagrange's theorem and it follows from the observation that $p|ab$ implies $p|a$ or $p|b$). Therefore, when $\left(\frac{a}{p}\right) = -1$ we must have that

$$a^{\frac{p-1}{2}} \not\equiv 1 \bmod p.$$

On the other hand, by Fermat's Little Theorem, we know $a^{p-1} \equiv 1 \bmod p$. So if we let $y \equiv a^{\frac{p-1}{2}} \bmod p$, then $y^2 \equiv 1 \bmod p$, so $y \equiv \pm 1 \bmod p$. Since $y \not\equiv 1 \bmod p$, then $y \equiv -1 \bmod p$, hence

$$a^{\frac{p-1}{2}} \equiv -1 = \left(\frac{a}{p}\right) \bmod p.$$

□

3 Preliminaries on Complex Numbers

A complex number, is a number of the form $a + bi$, where $i^2 = -1$.

We can add complex numbers:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

We can multiply complex numbers:

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

We can even divide them:

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \left(\frac{ac+bd}{c^2+d^2}\right) + \left(\frac{bc-ad}{c^2+d^2}\right)i.$$

For a complex number $a + bi$, we say the norm $N(a + bi)$ is $a^2 + b^2$.

Theorem 3. The Norm is a multiplicative function, i.e.,

$$N((a + bi)(c + di)) = N(a + bi) \cdot N(c + di).$$

Proof.

$$\begin{aligned} N((a+bi)(c+di)) &= N((ac-bd)+(ad+bc)i) \\ &= (ac-bd)^2 + (ad+bc)^2 \\ &= a^2c^2 + b^2d^2 - 2acbd + a^2d^2 + b^2c^2 + 2adbc \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2+d^2) + b^2(d^2+c^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &= N(a+bi) \cdot N(c+di). \end{aligned}$$

□

[1] Fermat's Little Theorem states that for $x \not\equiv 0 \bmod p$, we have $x^{p-1} \equiv 1 \bmod p$.

4 Preliminaries on Euclidean Algorithm

Theorem 4 (Division Algorithm)**.** Let a and b be positive integers. Then there exist unique integers q and r such that

- $a = bq + r$,
- $0 \le r < b$.

The Euclidean algorithm is an algorithm to find the greatest common divisor of two positive integers. It consists of repeatedly applying the division algorithm until one gets a remainder of 0:

Theorem 5 (Euclidean Algorithm)**.** Let a, b be positive integers with $a > b$. If $b|a$, then the greatest common divisor of a and b is b. Otherwise, we apply the division algorithm multiple times to get

$$\begin{aligned}
a &= bq_1 + r_1 && \text{with } 0 < r_1 < b \\
b &= r_1 q_2 + r_2 && \text{with } 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && \text{with } 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} q_n + r_n && \text{with } 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_{n+1}.
\end{aligned}$$

The greatest common divisor of a and b is r_n.

For the algorithm on sums of squares, we will need to adapt these last two theorems to complex numbers. In particular, we want to consider complex numbers of the form $a + bi$ with a and b integers. When a, b are integers, then $a + bi$ is called a Gaussian integer.

Theorem 6 (Division Algorithm for Gaussian Integers)**.** Let α and β be Gaussian integers. That is $\alpha = a+bi$ for some integers a, b and $\beta = c + di$ for some integers c, d. Then, there exist Gaussian integers γ and ρ such that

- $\alpha = \beta\gamma + \rho$,
- $0 \le N(\rho) \le \frac{1}{2}N(\beta)$.

Proof. We have

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \left(\frac{ac+bd}{c^2+d^2}\right) + \left(\frac{bc-ad}{c^2+d^2}\right) i.$$

Let q_1 be the nearest integer to

$$\left(\frac{ac+bd}{c^2+d^2}\right),$$

and q_2 is the nearest integer to

$$\left(\frac{bc-ad}{c^2+d^2}\right).$$

Now, let ε_1 be

$$\left(\frac{ac+bd}{c^2+d^2}\right) - q_1,$$

and ε_2 be

$$\left(\frac{bc-ad}{c^2+d^2}\right) - q_2.$$

Note $|\varepsilon_1| \le \frac{1}{2}$ and $|\varepsilon_2| \le \frac{1}{2}$.

Let $\gamma = q_1 + q_2 i$. Let $\rho = \alpha - \beta\gamma = (\varepsilon_1 + \varepsilon_2 i)\beta$. Then, using that the Norm is multiplicative (Theorem 3),

$$\begin{aligned}
N(\rho) &= N(\alpha - \beta\gamma) = N(\varepsilon_1 + \varepsilon_2 i) \cdot N(\beta) \\
&= (\varepsilon_1^2 + \varepsilon_2^2) N(\beta) \le \frac{1}{2} N(\beta).
\end{aligned}$$

□

With the Division algorithm for Gaussian integers in our back pocket we can easily define the Euclidean algorithm for Gaussian integers:

Theorem 7 (Euclidean Algorithm for Gaussian integers)**.** Let α, β be Gaussian integers.

$$\begin{aligned}
\alpha &= \beta\gamma_1 + \rho_1 && \text{with } 0 < N(\rho_1) \leq \frac{1}{2}N(\beta) \\
\beta &= \rho_1\gamma_2 + \rho_2 && \text{with } 0 < N(\rho_2) \leq \frac{1}{2}N(\rho_1) \\
\rho_1 &= \rho_2\gamma_3 + \rho_3 && \text{with } 0 < N(\rho_3) \leq \frac{1}{2}N(\rho_2) \\
&\vdots \\
\rho_{n-2} &= \rho_{n-1}\gamma_n + \rho_n && \text{with } 0 < N(\rho_n < \rho_{n-1} \\
\rho_{n-1} &= \rho_n\gamma_{n+1}.
\end{aligned}$$

The greatest common divisor of α and β is ρ_n.

Let's do a couple of examples:

Example 1:
Let's find the greatest common divisor of 13 and $5 + i$.

$$\begin{aligned}
13 &= 2(5 + i) + (3 - 2i) \\
5 + i &= (3 - 2i)(1 + i) + 0.
\end{aligned}$$

Therefore, the greatest common divisor is $3 - 2i$.

Example 2:
Let's find the greatest common divisor of 15485917 and $7378356 + i$.

$$\begin{aligned}
15485917 &= 2(t + i) + (729205 - 2i) \\
t + i &= 10(729205 - 2i) + (86306 + 21i) \\
729205 - 2i &= 8(86306 + 21i) + (38757 - 170i) \\
86306 + 21i &= 2(38757 - 170i) + (8792 + 361i) \\
38757 - 170i &= 4(8792 + 361i) + (3589 - 1614i) \\
8792 + 361i &= (361 - 8791i)(3589 - 1614i) + 0.
\end{aligned}$$

Therefore, the greatest common divisor is $3589 - 1614i$.

5 Algorithm

We are now ready to describe the Rabin-Shallit's algorithm.[2]

1. Pick a number b randomly such that $2 \leq b \leq p - 1$. Evaluate $x = b^{\frac{p-1}{2}} \bmod p$.
2. If $x \equiv 1 \bmod p$, then go back to step 1. Otherwise, $x \equiv -1 \bmod p$ and we can move on to Step 3.
3. Let $t \equiv b^{\frac{p-1}{4}} \bmod p$.
4. Using the Euclidean Algorithm for Gaussian integers, find the greatest common divisor of $t + i$ and p.
5. Suppose the greatest common divisor is $a + bi$. Then $a^2 + b^2 = p$.

[2]We made some modifications to Rabin-Shallit's algorithm to make some steps easier to understand for undergraduate students.

Let's prove the algorithm works.

When we pick b in the interval $[2, p-1]$, then by Fermat's Little Theorem $b^{p-1} \equiv 1 \bmod p$, so $b^{(p-1)/2} \equiv \pm 1 \bmod p$. From Euler's Criterion (Theorem 2), we know $b^{(p-1)/2} \equiv 1 \bmod p$ when b is a quadratic residue modulo p and $b^{(p-1)/2} \equiv -1 \bmod p$ when b is a quadratic non-residue modulo p. From Theorem 1 we know that for half the values of b, b is a quadratic residue and for half the values of b, b is a quadratic non-residue. Therefore, with probability 1/2 [3], we get $b^{(p-1)/2} \equiv -1 \bmod p$.

Once we have $b^{(p-1)/2} \equiv -1 \bmod p$, then $t \equiv b^{(p-1)/4}$ satisfies $t^2 \equiv b^{(p-1)/2} \equiv -1 \bmod p$. Therefore t^2+1 is a multiple of p. If we write $t^2+1 = mp$, we have that $t^2+1 \leq (p-1)^2+1 < p^2$, so $m < p$. Therefore m is not a multiple of p.

Suppose $d = a + bi$ is the greatest common divisor of $t + i$ and p. Then $N(d)|N(t+i) = mp$ and $N(d)|N(p) = p^2$. Since $mp < p^2$, we have that $N(d)$ is 1 or p (the positive integer divisors of p^2 are $1, p, p^2$). It turns out that when p is a prime congruent to 1 modulo p, then $p = \pi \cdot \bar{\pi}$. Then $\pi|p$ and $\pi|t^2+1 = (t+i)(t-i)$. If $\pi|t-i$, then $\bar{\pi}|\overline{t-i} = t+i$. Therefore, there is a divisor of $t+i$ that also divides p. That means $N(d) > 1$. Therefore $N(d) = p$. But that implies $a^2 + b^2 = p$.

6 Running Time Analysis

Let's analyze how long the algorithm takes. To evaluate $b^{(p-1)/2} \bmod p$ we can use the fast exponentiation modular algorithm that has $O(\log p)$ multiplications. Now, because the probability that $b^{(p-1)/2} \equiv -1 \bmod p$ is around 1/2, it means on average we just need to check two values of b. Therefore, on average, it takes $O(\log p)$ multiplications to get to Step 3 of the algorithm.

To evaluate $b^{(p-1)/4} \bmod p$ we have $O(\log p)$ operations. To evaluate the greatest common divisor, we do $O(\log p)$ operations (note that the norm drops by half each time the division algorithm is performed, that is why we only need $O(\log p)$ multiplications).

Therefore, the algorithm has $O(\log p)$ multiplications.

7 Examples

1. Suppose we want to find two integers whose squares add up to 13. After checking $b^6 \bmod 13$ for some random elements we find that $t \equiv 5 \bmod 13$. Then we find the greatest common divisor of $t+i$ and 13 and get $3-2i$. Therefore $3^2+2^2 = 13$.

2. Suppose we want to find two integers whose squares add up to 15485917. After checking $b^{(15485917-1)/2} \bmod 15485917$ for some random elements we find that $t \equiv 7378356 \bmod 15485917$. Then we find the greatest common divisor of $t+i$ and 15485917 and get $3589 - 1614i$. Therefore $3589^2 + 1614^2 = 15485917$.

References

[1] Michael O. Rabin and Jeffery O. Shallit, *Randomized algorithms in number theory*, vol. 39, 1986, Frontiers of the mathematical sciences: 1985 (New York, 1985), pp. S239–S256. MR 861490

[3] technically, the probability is slightly higher since we are excluding $b = 1$.