Writing primes as the sums of squares

Christopher Lutsko

Abstract

When teaching introductory number theory, one of my favorite questions to answer is *When can we write a prime as the sum of two squares?* and *How?* I think the proof presented here is particularly nice as it combines the Gaussian integers (in particular the Euclidean algorithm), quadratic residues, and Euler's criterion in the proof. Moreover, this problem clear demonstrates that these more esoteric number theoretic objects (Gaussian integers, congruences) are not just intrinsically interesting, but offer one tools to study the rational integers. Also on my website is a short mathematica file which can be used to impress your friends and family by expressing large primes as the sum of two squares.

First, we have the following exercise

Exercise 1. *If $p \equiv 3 \pmod 4$ then p cannot be written as the sum of two squares.*

Moreover, we know that $2 = 1^2 + 1^2$ *can* be written as the sum of two squares. This leaves the primes of the form $p \equiv 1 \pmod 4$. Our main theorem for this note is then

Theorem 1. *Every prime $p \equiv 1 \pmod 4$ is the sum of 2 squares.*

Proof. The proof will follow an algorithmic construction, which we can actually use to write any prime as the sum of two squares. Fix a prime p.

`[Step 1]`: Find a quadratic non-residue of p. Recall that half of the residues modulo p are non-residues. Thus, we simply test $a^{\frac{p-1}{2}}$, if $a^{\frac{p-1}{2}} \equiv -1 \pmod p$ then we have found a quadratic non-residue by Euler's criterion.

`[Step 2]`: Set $z = \sqrt{a^{\frac{p-1}{2}}} = a^{\frac{p-1}{4}}$. Note that z is an integer since $p \equiv 1 \pmod 4$. Therefore $z^2 + 1 \equiv 0 \pmod p$.

Thus, we there exists a $k \in \mathbb{Z}^{\neq 0}$ such that $z^2 + 1 = p \cdot k$. Now, in the Gaussian integers, we may factor $z^2 + 1$ giving

$$(z + i)(z - i) = p \cdot k.$$

[Step 3]: Now, in the Gaussian integers p may not be a prime. Therefore, use the Euclidean algorithm to find the gcd of $z+i$, and p which we call d, and write $z+i = de$ and $z-i = \overline{d}\overline{e}$.

Since $pk = (z+i)(z-i) = de\overline{d}\overline{e}$ it must be the case that $p = d\overline{d}$ (since otherwise there is a f which divides p and $e\overline{e}$, and therefore, an f' which divides p and e which is a contradiction). Thus $p = |d|^2 = N(d)$ (the norm of d). But the norm of d is exactly the sum of two squares! □

Let us see an example. Note that $37 = 36 + 1 \equiv 1 \pmod 4$.

[Step 1]: Find a quadratic non-residue mod 37. $2^{18} \equiv -1 \pmod{37}$ therefore 2 is a quadratic non-residue.

[Step 2]: Set $z = 2^9 = 512 \equiv 31 \pmod{37}$. Thus, we have $z^2 + 1 \equiv 0 \pmod{37}$ which we can write as $(z+i)(z-i) = 37k$ for k a nonzero integer.

[Step 3]: Now we use the Euclidean algorithm to find the gcd of $31+i$ and 37:

$$\frac{37}{31+i} = 1 + \frac{185}{962} - \frac{37}{962}i \qquad \Longrightarrow \qquad 37 = 1 \cdot (31+i) + (6-i)$$

$$\frac{31+i}{6-i} = 5 + i \qquad \Longrightarrow \qquad 31 + i = (6-i) \cdot (5+i) + 0$$

therefore the gcd is $6-i$. Now note that $N(6+i) = 6^2 + 1^2 = 37$.

Exercise 2. *Write* 193 *as the sum of two squares. (Hint:* $5^{96} \equiv -1 \pmod{193}$ *and* $5^{48} \equiv 112 \pmod{193}$*).*

Note that WolframAlpha and Mathematica can do modular arithmetic, and can find the GCD of Gaussian integers. Thus, we can write, even very large primes, as the sums of two squares in a few lines of code.

Exercise 3. *Write a program to write the* n^{th} *prime as the sum of two squares (if this is possible).*

Department of Mathematics, Rutgers University, Hill Center - Busch Campus, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019, USA. *E-mail:* ***chris.lutsko@rutgers.edu***