UW Math Circle
March 26, 2020

# Number theory problems

To prove Fermat's two square theorem, we relied on two facts:

**Theorem 1 (Wilson's theorem)** *If $p$ is prime, then $(p-1)! \equiv -1$ mod $p$.*

**Lemma 1 (Lagrange's lemma)** *If $p$ is prime and $p \equiv 1$ mod 4 is prime, then there exists an integer $m$ such that $p|m^2+1$.*

It's now your job to prove these two facts! The following steps will walk you through it.

Let's start with a quick review of modular arithmetic. Using mod 5, for example, means that means we call two numbers equivalent if their difference is a multiple of 5. For example, $12 \equiv 2 \bmod 5$ because $12 - 2 = 10$ is a multiple of 5. Mods are nice because they preserve addition and multiplication: for any integers $a, b, c, d$,

$$a \equiv b \bmod c \implies a + d \equiv b + d \bmod c, \text{ and } ad \equiv bd \bmod c.$$

Now to the proofs:

1. Let $p$ be prime. Fix an integer $1 \leq x \leq p-1$, and consider the list

   $$x \bmod p, 2x \bmod p, 3x \bmod p, \ldots, (p-1)x \bmod p.$$

   Prove that all the numbers in this list are different, and that none of them are 0.

2. Conclude that every integer $1 \leq x \leq p-1$ has a unique inverse mod $p$, i.e. there exists a unique number $x^{-1}$ such that $x^{-1}x \equiv 1 \bmod p$.

3. Check that $1! \equiv -1 \bmod 2$ and $2! \equiv -1 \bmod 3$.

4. Suppose $p > 3$ is prime. Show that you can group the numbers $2, 3, \ldots, (p-2)$ into pairs so that the product of each pair is 1. Use this to complete the proof of Wilson's theorem. (Hint: use your work from part 1.)

5. Applying Wilson's theorem directly to $p = 4k+1$ gives

   $$(4k)! \equiv -1 \bmod p. \tag{1}$$

   Show that $(4k)! \equiv (2k)!^2 \bmod p$ by re-grouping the terms of $(4k)!$ in a special way.

6. Conclude that $p|(2k)!^2 + 1$.

Bonus: What is $(p-1)!$ mod $p$ if $p$ is not prime?

**Gaussian Integers**

We also used the fact that Gaussian integers can always be factored into primes. Let's explore the Gaussian integers/primes a little more...

If $z$ and $w$ are Gaussian integers, we say $z$ divides $w$ if there exists a Gaussian integer $u$ such that $w = u \cdot z$. There are some special numbers in the Gaussian integers, that we call **units**: they are the Gaussian integers of norm 1, i.e. $1, -1, i$ and $-i$. The units are special because they divide everything!

A Gaussian integer $z$ is called a **G-prime** (Gaussian prime) if it cannot be written as $z = x \cdot y$ for some Gaussian integers $x, y$, with neither $x$ nor $y$ a unit.

Regular primes may not be Gaussian primes: for example, 5 is prime, but not G-prime, because $5 = (1 + 2i)(1 - 2i)$. Proving that Gaussian integers are G-prime can be a tricky business. One useful tool is the norm, $N(a + bi) = a^2 + b^2$.

Some problems:

a. Prove that $N((a + ib) \cdot (c + di)) = N(a + ib) \cdot N(c + di)$ by doing all the multiplications.

b. Let $z$ denote a Gaussian integer. Use part a to show that if $N(z)$ is prime, then $z$ is G-prime.

c. Show that $1 + i$ is prime.

d. Show that $N(z)$ is even if and only if $1 + i|z$.

e. Show that 2 is not prime by factoring it.

f. List all G-primes that have norm less than 10. How many are there?

g. Show that 3 is prime. Note that the norm of 3 is 9, so you can't use the test from part b!

h. Determine which of the following are G-prime: $1+3i, 3+4i, 14-5i, 53$. If it isn't G-prime, find a factorization into G-primes.

i. Note that $5 = (1+2i)(1-2i) = (2+i)(2-i)$. Why doesn't this violate unique factorization?

Harder problems:

- Show that if $p$ is a prime and $p \equiv 1 \bmod 4$, then there is a unique pair of integers $a, b$ such that $a^2 + b^2 = p$. (Hint: suppose there are two different pairs, and try to derive a contradiction using prime factorization over the Gaussian integers.)
- For which odd numbers $n$ is $n + i$ G-prime?
- Show that if $p$ is a prime and $p \equiv 3 \bmod 4$, then $p$ is G-prime. (Hint: start by showing that there is no Gaussian integer $z$ with $N(z) \equiv 3 \bmod 4$.)
- Suppose $N(z)$ is a square number (1, 4, 9, 16, etc). Does there necessarily exist a Gaussian integer $w$ with $z = w^2$? Prove that this is always true, or find a counterexample.