Math 25 – Group Programming Assignment $3i$

Due Tuesday, November 15th, *beginning of class.*

1. Find an odd prime p such that every element of $\{-100, \ldots, 100\}$ is a square modulo p.

   Remark: You'll probably want to use an `is_prime` function from a library.

   Solution: Let S denote the set of odd primes in the interval $[3, 100]$. We first construct a prime p which satisfies the congruences

   $$p \equiv 1 \pmod 8, \quad p \equiv 1 \pmod q \quad \text{for all } q \in S.$$

   In other words, denote $N := 8 \prod_{q \in S} q$. We are looking for a prime of the form

   $$p = kN + 1$$

   for some k. Using Sage's `is_prime` function and a bit of trial and error

```
S = [x for x in range(3, 100) if is_prime(x)]
N = 8 * prod(S)
assert is_prime(5*N + 1)
```

   we may choose $k = 5$ and let $p = 5N + 1$.

   We now prove that the numbers $-100, \ldots, 100$ are all quadratic residues modulo p. It is easy enough to verify this by computer and Euler's criterion.

```
p = 5*N + 1
s = (p-1) // 2
assert {pow(x, s, p) for x in range(-100, 101) if x != 0} == {1}
# By Euler's criterion, every element of the set above is a quadratic residue.
# Trivially 0 is always a square.
```

   However, this does not illuminate exactly why we've constructed p as we did. The following is a better explaination.

   We have insisted that $p \equiv 1 \pmod 8$, so by the first and second supplements to quadratic reciprocity

   $$\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) = 1.$$

   Additionally, by quadratic reciprocity we have for the primes $q \in S$ that

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

   since $p \equiv 1 \pmod q$. Finally, let $a \in \{-100, \ldots, 100\}$ be nonzero and let

   $$a = (-1)^x 2^y \prod_{q \in S} q^{e_q}$$

   be its prime factorization (where e_q is allowed to be 0). Then by multiplicativity of the Legendre symbol

   $$\left(\frac{a}{p}\right) = \left(\frac{(-1)^x 2^y \prod_{q \in S} q^{e_q}}{p}\right) = \left(\frac{(-1)^x}{p}\right) \cdot \left(\frac{2}{p}\right)^y \cdot \prod_{q \in S} \left(\frac{q}{p}\right)^{e_q} = 1.$$

   Thus every $-100 \leq a \leq 100$ is a square mod p (including, trivially, 0).

2. We now finally solve the problem from the syllabus page. First, one notices by inspection that

$$(-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3 = 42.$$

(Credit of course to Booker and Sutherland. This took...a while to find.)

It is much easier to prove that $40, 41$ are *not* the sum of three cubes. Prove this. (Hint: look mod 9.)

Solution: First we prove that if n is a sum of three integer cubes, then

$$n \equiv 0, 1, 2, 3, 6, 7, 8 \pmod 9.$$

This is just a matter of enumerating the cases.

```
import itertools
sums = {(x^3 + y^3 + z^3) % 9 for x,y,z in itertools.product(range(9), repeat=3)}
assert sums == {0, 1, 2, 3, 6, 7, 8}
```

We see that $40 \equiv 4 \pmod 9$ and $41 \equiv 5 \pmod 9$, so cannot be the sum of three cubes.

3. (Advanced topics) Prove that for any $k \in \mathbb{N}$, there exists an odd prime p such that each $x \in \{-k, \ldots, k\}$ is a quadratic residue modulo p. One might find Dirichlet's theorem on primes in arithemtic progressions helpful.

4. (Advanced topics, Advertisement)

Recall from the solutions of assignment 3 the following remark:

Remark. *It is presently unknown whether a 3×3 magic square of squares with integer entries exists. It is also "unknown" whether a 3×3 magic square of squares with entries in $\mathbb{Z}/n\mathbb{Z}$ exists for all sufficiently large n. See `https://www.youtube.com/watch?v=FCczHiXPVcA`.*

Now, Voight and I were thinking that settling the $\mathbb{Z}/n\mathbb{Z}$ version of the question might be a nice prelude to an undergraduate research problem. If you find yourself drawn to the question, you could give the following an attempt:

Find a magic square of squares modulo 71. (Allegedly this exists.)

Comments about grading

See computing assignment 1.