2014-02-28-quad_reciprocity-1.sagews

February 28, 2014

Contents

1 Lecture: Quadratic Reciprocity (part 1) 2014-02-28

1.1 Introduction: A Surprising Pattern Involving Squares Modulo p

Question: For which primes is 4 a square modulo p?

Answer: All primes, obviously.

Question: When is 2 a square modulo p?

Lets make a table:

```
for p in primes(3, 100):
    print p, is_square(Mod(2,p))
```

```
3 False
5 False
7 True
11 False
13 False
17 True
19 False
23 True
29 False
31 True
37 False
41 True
43 False
47 True
53 False
59 False
61 False
67 False
71 True
73
```

```
True
79 True
83 False
89 True
97 True
```

```
for p in primes(3, 100):
    print p, p%8, is_square(Mod(2,p))
```

```
3 3 False
5 5 False
7 7 True
11 3 False
13 5 False
17 1 True
19 3 False
23 7 True
29 5 False
31 7 True
37 5 False
41 1 True
43 3 False
47 7 True
53 5 False
59 3 False
61 5 False
67 3 False
71 7 True
73 1 True
79 7 True
83 3 False
89 1 True
97 1 True
```

Question: When is 3 a square modulo p?

```
for p in primes(3, 100):
    print p, p%12, is_square(Mod(3,p))
```

```
3 3 True
5 5 False
7 7 False
11 11 True
13 1 True
17 5 False
19 7 False
23 11 True
29 5 False
31 7 False
37 1 True
41 5 False
43 7 False
47 11 True
```

```
53 5 False
59 11 True
61 1 True
67 7 False
71 11 True
73 1 True
79 7 False
83 11 True
89 5 False
97 1 True
```

This pattern is frankly really amazing

Surprising (Nontrivial) Theorem: Whether or not a is a square modulo (an odd prime) p only depends on p modulo $4a$.

Definition: The Legendre Symbol.

Let a be an integer and p an odd prime. Let

$$\left(\frac{a}{p}\right) = \begin{cases} 0\text{if } ngcd(a,p)nneq1, \\ +1\text{if } a \text{ is a quadratic residue, and} \\ -1\text{if } a \text{ is a quadratic nonresidue.} \end{cases}$$

The above theorem is the statement that $\left(\frac{a}{p}\right)$ only depends on the residue of p modulo $4a$.

```
for p in primes(3, 100):
    print p, p%12, legendre_symbol(3, p)
```

```
3 3 0
5 5 -1
7 7 -1
11 11 1
13 1 1
17 5 -1
19 7 -1
23 11 1
29 5 -1
31 7 -1
37 1 1
41 5 -1
43 7 -1
47 11 1
53 5 -1
59 11 1
61 1 1
67 7 -1
71 11 1
73 1 1
79 7 -1
83 11 1
89 5 -1
97 1 1
```

1.2 The Legendre Symbol and a Group Homomorphism

For any odd prime p, consider the map

$$\psi : \mathbf{F}_p^* \to \pm 1$$

given by $\psi(a) = \left(\frac{a}{p}\right)$.

Proposition: ψ is a surjective group homomorphism, i.e., $\psi(ab) = \psi(a)\psi(b)$, and -1 is in the image.

But, in order to prove this proposition, well need another Theorem, which we skipped from chapter 2:

Theorem: The group $\mathbf{F}_p^*$ is cyclic, i.e., there is an element $g \in \mathbf{F}_p^*$ such that every element of $\mathbf{F}_p^*$ is a power of g.

We will prove this theorem soon.

Incidentally, lets look at how often 3 is a generator modulo p:

```
for p in primes(5,1000):
    if Mod(3,p).multiplicative_order() == p-1:
        print p,
```

```
5 7 17 19 29 31 43 53 79 89 101 113 127 137 139 149 163 173 197 199 211 223 233 257 269
281 283 293 317 331 353 379 389 401 449 461 463 487 509 521 557 569 571 593 607 617 631
641 653 677 691 701 739 751 773 797 809 811 821 823 857 859 881 907 929 941 953 977
```

Wow, thats pretty often!

Unsolved Problem (Artins Primitive Root Conjecture): Prove that 3 is a generator of $\mathbf{F}_p^*$ for infinitely many primes p.

Note: You can replace 3 by any positive non-square, and the problem is still unsolved. It is implied by the (generalized) Riemann Hypothesis.

1.3 Gausss Law of Quadratic Reciprocity

The big theorem were aiming for is the following:

Theorem (Gauss) Suppose p and q are distinct odd primes. Then

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

Also

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \qquad \text{and} \qquad \left(\frac{2}{p}\right) = \begin{cases} 1 \text{ if } p \equiv \pm 1 \pmod 8 \\ -1 \text{ if } p \equiv \pm 3 \pmod 8. \end{cases}$$

Equivalent Questions:

- Is 5 a square modulo 2017? (Seems hard to answer by hand doesnt it!)
- Is 2017 a square modulo 5? (Not so bad)
- Is 2 a square modulo 5? (Really easy)
- Nope.

On the whiteboard, prove that

- $nmathbfF\_p^*$ is cyclic
- ψ is a homomorphism