2014-02-28-quad_reciprocity-1.sagews

February 28, 2014

Contents

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

- video: `http://youtu.be/uhBCb9-ET8M`

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:

```
a = randrange(0,10^1000); a
```

```
234131136588449060873601677667290274897762849367304691032360123886488691045739474392561229
```

```
234131136588449060873601677667290274897762849367304691032360123886488691045739474392561229
944863885921413510403325564574705185464962061647349669331743544870267181195141923333021749
131191236955633031637711891677634317079400582397378954426683982644835809733220344185736518
038365048019304608243444916280933947156250996980028529756449511853960197469675408498547040
697112275095390057568876812731170535945588149040784718831599419125833063330842817101407790
536395428297463225892534867467032451650109247896520927320821257569448350567331122967243133
358910416050452061952525181400719597954234699236037844960968130641162291690338295664019375
713311451776851889407384036599511363874583887181982280595181541056134520919060175448301648
385669522339932393614135480780945438871711009933279631654276393363127968266811804869041057
950093462401704706031405875999012888126186253790613153308305490061443664066539450243312787
484226024295001992898075523317317259312307476954874342572401067605211021687021369279389256
9634241871L
```

```
N(sqrt(a), digits=1000)
```

```
4.8387099167903117942083692204813064628471666265158893428566207674061287609437980199630495
```

```
636428865575837985556442632138542561157370078534816546029824210674515496091571868967646978
313987466428024283804711806094278652403791812137108368166066993361782915421175928711980297
280681283187649298134839663324254344045144111070243309635958753489475082046450949060053073
174322623826830856033300311510951382517908361959919908176171949568822565832405517287408677
962063407796332721910107926378761468329377732812561434712234063291001917157646918971365107
056100671084636251768492204350209938037126749151497234751731587160990976886371443784816231
010307175080995033318899472556203916466739811184657971347859635561689052642665441905223398
54508386099e499
```

```
q = next_probable_prime(10^1000); q
```

```
100000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000453
```

```
Is 2 a square modulo q?  NO
(Yes -- you can decide.)

Is 3 a square modulo q?  YES  -- but no idea what its square root is!
```

```
q%8
```

```
5
```

```
q%12
```

```
1
```

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

```
for p in primes(5, 100):
    print p, p%12, is_square(Mod(3,p))
```

```
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
```

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

Question: When is 3 a square modulo p?

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

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

$$\left(\frac{a}{p}\right) = \begin{cases} 0\text{if } ngcd(a,p)nneq1, \\ +1\text{if } a \text{ is a quadratic residue (=a square), and} \\ -1\text{if } a \text{ is a quadratic nonresidue (=not a square).} \end{cases}$$

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p$$

```
Mod(2,q)^((q-1)/2)
```

```
1000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000452
```

```
Mod(3,q)^((q-1)/2)
```
1

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)
```

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(5,4000):
    if Mod(3,p).multiplicative_order() == p-1:
        print p,
```

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