Math 215 Spring 2023 Number Theory II

Sums of Squares ; Applications of Quadratic Reciprocity

Sankar Sitaraman – nature-lover.net/math

Math Dept, Howard University

1-11-2023

Outline

Few facts about Fermat Numbers

A fermat number F_n for $n = 1, 2, 3, ...$ is an integer of the form

$$F_n = 2^{2^n} + 1.$$

Basic facts:
All fermat numbers are sums of squares !

HW1, problem 1 : If $2^m + 1$ is prime, show that m is a power of 2.

The first four are primes:
$F_1 = 3, F_2 = 17, F_3 = 257, F_4 = 65537.$
No other Fermat prime is known!

It is still possible that infinitely many are prime!

Lucas' theorem on Fermat numbers

Let $n \geq 2$. Then Lucas proved that

$$p | F_n \implies p \equiv 1 \pmod{2^{n+2}}$$

This makes it easier to find factors of Fermat numbers.

It also gives us some big prime numbers, because each such prime is of form $k2^m + 1$!

Proof of Lucas' theorem : Sketch

1. Start by noting that
$$p|F_n \implies 2^{2^n} \equiv -1 \pmod{p}.$$
2. Show that, if $p|F_n$, then the *multiplicative order* of 2 $\pmod{p}$ is 2^{n+1}. See next page for proof.
3. **HW1, Problem 2** Show that, for such p we have 2 is a quadratic residue mod p.
4. Show that, if $2 \equiv x^2 \pmod{p}$ then the *multiplicative order* of $x \pmod{p}$ is 2^{n+2}.
5. Conclude that 2^{n+2} divides $p-1$ and hence $p \equiv 1 \pmod{2^{n+2}}$

Proof that $o(2) = 2^{n+1}$.

Proof that multiplicative order of 2 mod p is 2^{n+1}.

First note the following:

$$2^{2^n} \equiv -1 \pmod{p} \implies \left(2^{2^n}\right)^2 = 2^{2^{n+1}} \equiv 1 \pmod{p}.$$

Let $m = o(2)$ be the order mod p where $p|F_n$ and suppose $m < 2^{n+1}$.

Now, order of an element a always divides any k such that $a^k \equiv 1 \pmod{p}$.
You can check this by writing $k = qm + r$ using Euclidean algorithm and then looking at a^k. If k doesn't divide m then $r < m$ and you get $a^m \equiv 1$ which is a contradiction.
So $m|2^{n+1} \implies m = 2^d, d < n+1$. But then you get $2^m \equiv 1 \implies 2^{2^t} \equiv 1$ for all $t \geq d$ by successive squaring. Thus you can't have $2^{2^n} = -1$, a contradiction.

Basic properties of $n^2 + 1$

1. $n^2 + 1$ is a sum of two squares!
2. It is conjectured that there are infinitely many primes of this form.
3. Best result: Fouvry and Iwaniec (1997) proved using sieve methods that there are infinitely many primes of type $p = l^2 + m^2$ where l is a prime number.

Some facts about $n^2 + 1$

1. If a prime p divides $n^2 + 1$ then it is either 2 or of form $4m + 1$.
   Idea: Use quadratic reciprocity: Why is -1 is a square mod p?
2. If a prime $p = a^2 + b^2$, then we can compute k such that p divides $k^2 + 1$.
   Idea: Look at $a^2 + b^2 \equiv 0 \pmod{p}$ and "divide" by b on both sides.

When is a prime a sum of two squares?

Question: When is a prime a sum of squares of two integers? Assume $p > 2$. If $p = 2$ we have $2 = 1^2 + 1^2$.

1. Easy: If $p = a^2 + b^2$ then as above, $x^2 + 1 \equiv 0 \pmod{p}$ has a solution. This means -1 is a square mod p and thus $p \equiv 1 \pmod{4}$.
2. Difficult: If $p = 4m + 1$ for some m, we can write $p = a^2 + b^2$.
3. Known: If $p = 4m + 1$ then -1 is a quadratic residue mod p and $x^2 + 1 = kp$ for some p.
4. Actually we know one solution: $((p-1)/2)! \pmod{p}$ (using Wilson's theorem).

When is a prime a sum of two squares? Proof outline

Given $p = 4m + 1$ when is it a sum of two squares?

Proof using Gaussian integers:
(Reference: Herstein, Topics in Algebra)
Know: -1 is a quadratic residue mod p and $x^2 + 1 = kp$ for some p.

1. Show that k can be chosen to be prime to p.
2. Show that p is not prime in $\mathbb{Z}[i]$
3. If $p = (a + bi)(c + di)$ neither being a unit, show that $p = a^2 + b^2$ or $p = c^2 + d^2$.

Facts about Gaussian Integer ring

As soon as we have a Euclidean norm and Euclidean algorithm in an integral domain, we get a Euclidean domain.
A Euclidean domain is a PID (principal ideal domain) and hence a UFD (unique factorization domain). Proof is very similar to the case in the ring of integers.
So we see that these rings share a lot in common with integers. You can factor, divide, get remainders, find GCD etc just like you would in the ring of integers.

Facts about Gaussian Integers

Facts about Gaussian integers:

1. Gussian Integers are UFDs
2. Every prime element is also an irreducible element.
3. The norm is $a^2 + b^2$ for every $a + bi$ and it is multiplicative.
4. Using multiplicativity of norm, we can show that an element is a unit iff its norm is 1.
5. The only units are $1, -1, i, -i$ and they form a subgroup. This follows from $a^2 + b^2 = 1$.
6. Also using multiplicativity of norm, we can show that if the norm of an element is prime then it is a prime integer in $\mathbb{Z}[i]$. But the converse is not true Will talk about this more later in these notes.

Factorization, Irreducibles and primes etc in other number rings

It was thought at one time that all rings obtained using roots of unity (for example Gaussian integers are obtained using i, a fourth root of unity) are UFDs, and a proof of Fermat's last theorem was proposed by Lamé under this assumption. Kummer showed this is false. The smallest example where it fails to be UFD is $\mathbb{Z}[\zeta_{23}]$ where ζ_{23} is a "primitive" 23rd root of unity (meaning its multiplicative order is 23).

Facts about Irreducibles and Primes

1. Every prime element in any integral domain is also irreducible :
   $p = ab \implies p|a$ or $p|b$ so $pk = a$ or $pk = b$ for some k. So we get $p = pka$ or $p = pkb$. Get that $1 = ka$ or $1 = kb$ which means a or b is a unit. So p is irreducible.
2. In any UFD irreducible elements are also prime. This is easily seen using unique factorization.
3. $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. Other examples are $\mathbb{Z}[\sqrt{10}]$ and $\mathbb{Z}[\sqrt{-3}]$.
4. In $\mathbb{Z}[\sqrt{-5}]$ we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$.

Factorization, Irreducibles and primes etc in other number rings -2

Facts about Irreducibles and Primes (contd) :

1. The norm in $\mathbb{Z}[\sqrt{-5}]$ is $a^2 + 5b^2$. Taking norm of both sides, show that $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$ is not possible. Similarly for 3.
2. Show that 2 and 3 are irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$

When is a prime a sum of two squares? Proof

Given $p = 4m+1$ is it a sum of two squares?

Know: -1 is a quadratic residue mod p and $x^2+1 = kp$ for some p. In fact x can be picked so that $x < p/2$ because there are two roots, one of them below $p/2$ and its negative above $p/2$.

1. k can be chosen to be prime to p : (will show $1 \leq k < p$)

$$kp = x^2+1 \implies kp \leq \frac{p^2}{4}+1 < \frac{p^2}{2} \implies k < p/2 < p.$$

2. p is not prime / irreducible in $\mathbb{Z}[i]$:
Suppose p were prime.

$$x^2+1 = kp \implies (x+i)(x-i) = kp$$

$$\implies p|(x+i) \text{ or } p|(x-i) \implies p|1 \quad \textit{impossible}$$

When is a prime a sum of two squares? Proof conclusion

Given $p = 4m + 1$ is it a sum of two squares?

1. So $p = (a + bi)(c + di)$ with neither factor being a unit. Taking norm we get $p^2 = (a^2 + b^2)(c^2 + d^2)$. Since neither factor is unit neither of their norms is 1 so $p = a^2 + b^2 = c^2 + d^2$. In fact we will have $p = (a + ib)(a - ib)$.

What numbers are sums of two squares?

1. In a number ring, if norm of an element is prime then the element is prime itself.
2. In $\mathbb{Z}[i]$ the primes p that are 2 or of form $4n+1$ factor into two primes $u+iv$ and $u-iv$ because $p = u^2+v^2$ and so it is the norm of these elements.
   The primes of form $4n+3$ do not:
   Proof: Suppose $p = (u+iv)(w+iz)$ then taking norm $p^2 = (u^2+v^2)(w^2+z^2)$ with neither a unit. From this you get $u^2+v^2 = w^2+z^2 = p$ which is not possible because only primes that are 1 mod 4 can be sum of two squares. Thus primes of form $4n+3$ are prime elements even in the ring of Gaussian integers.

What numbers are sums of squares?- page 2

1. If $n = a^2 + b^2 = (a + bi)(a - bi)$ then any prime p of form $4n + 3$ dividing n either divides $a + bi$ or $a - bi$
   Then it divides both real and imaginary parts a and b so it also divides $a - bi$ and thus p^2 divides n also.
2. So after dividing by p^2 you can now look at n/p^2 and this is the sum of two squares: namely the squares of a/p and b/p.

What numbers are sums of squares? - page 3

1. Continuing like this we get some m which is sum of two squares but has no prime factors of form $4n+3$. Thus all of its factors are either 2 or primes of form $4n+1$.
2. Thus $n = p_1 p_2 ... p_k M^2$ where p_i are 2 or of form $4n+1$.

In the book they start with product of primes of the form $4n+1$ and thus of form u^2+v^2.
As we saw before,
$(u^2+v^2)(w^2+z^2) = (uw+vz)^2 + (vw-uz)^2$. So any product of such primes is also a sum of two squares.
Then looking ar the common factors of a and b in a^2+b^2 they prove that $n = p_1 p_2 ... p_k M^2$ where p_i are 2 or of form $4n+1$.

What numbers are sums of squares? - page 4

Theorem: If $m = a^2 + b^2$ with $gcd(a, b) = 1$ then :
2) m is odd and a product of primes that are 1 mod 4 or equal to 2.
3) m is even and $m/2$ is a product of primes that are 1 mod 4 or equal to 2.
On the other hand if the requirement $gcd(a, b) = 1$ is dropped then $m = a^2 + b^2$ iff $m == p_1 p_2 ... p_k M^2$ where p_i are 2 or of form $4n + 1$.

We have seen how to prove this with Gaussian integers. The key, as we saw, is that primes that are 3 mod 4 when they divide $a^2 + b^2$ they end up dividing both a and b.
For the proof, without using Gaussian integers,

What numbers are sums of squares? - conclusion

For the proof, without using Gaussian integers, the following two ideas might help:
1) If $m = a^2 + b^2$ and a prime divisor of m, say p, doesn't divide a or b then we get a solution for $x^2 \equiv -1 \pmod{p}$. This means $p \equiv 1 \pmod{4}$. If on the other hand, a prime divisor of m, say p, divides a and b then p^2 also divides $a^2 + b^2$.
2) Product of two sums of squares is itself a sum of two squares.

What numbers are sums of squares? - conclusion

For the proof, without using Gaussian integers, the following two ideas might help:
1) If $m = a^2 + b^2$ and a prime divisor of m, say p, doesn't divide a or b then we get a solution for $x^2 \equiv -1 \pmod{p}$. This means $p \equiv 1 \pmod{4}$. If on the other hand, a prime divisor of m, say p, divides a and b then p^2 also divides $a^2 + b^2$.
2) Product of two sums of squares is itself a sum of two squares.

Pythagorean triples and sums of two squares

Recall the following parametrization for all primitive Pythagorean triples:

$$\text{Given odd integers } s > t \geq 1,\ gcd(s,t) = 1,$$

$a = st, b = \frac{s^2 - t^2}{2}, c = \frac{s^2 + t^2}{2}$ is a primitive Pythagorean triple

Based on the theorem we just discussed, we get that $2c = s^2 + t^2$ with c odd iff c is a product of primes that are 1 mod 4. [c has to be odd or else 4 will divide $s^2 + t^2$ and show this is impossible if s, t are odd].

More about primes in Gaussian integers

Recall that, if the norm of a Gaussian integer is prime, then it is a prime itself.
But the converse is not true. If $p \equiv 3 \pmod 4$ then $Norm(p) = p^2$ but we will see that p is a prime *as a Gaussian integer* as well:

Among Gaussian integers, there are 3 types of primes, *upto multiplication by units:*
(1) $1 + i$ or $1 - i$, both of norm 2.
(2) The integer primes $p \equiv 3 \pmod 4$, of norm p^2.
(3) The elements $u + iv$ of norm p such that $u^2 + v^2 = p$, where p is a prime integer. Such p will have to be congruent to 1 mod 4, as we have shown above.

The nature of primes in Gaussian integers - page 1

It is easy to show that $1+i, 1-i$ are primes. In fact, their norm is a prime, so we are done.
If $p \equiv 1 \pmod 4$ then $p = u^2 + v^2$ for some u, v with $gcd(u, v) = 1$ and $u + iv$ and $u - iv$ are primes because they are of norm p.
If $p \equiv 3 \pmod 4$ then p cannot be sum of two squares. Is p a Gaussian prime? Suppose not. Then $p = (a + ib)(c + id)$ *where neither factor is a unit* and taking norms,
$p^2 = (a^2 + b^2)(c^2 + d^2)$ where we must have
$a^2 + b^2 = p, c^2 + d^2 = p$ since neither is a unit. But $p \equiv 3 \pmod 4$ so it cannot be a sum of two squares.
So p is a prime of norm p^2.

The nature of primes in Gaussian integers -page 2

Now we prove the converse. Given a Gaussian prime, we show it is one of the above. We use the fact that if a prime element in any ring divides a product then it divides one of the factors.

Suppose α is a Gaussian prime, $\alpha = a + ib$, and
$Norm(\alpha) = \alpha\overline{\alpha} = N = a^2 + b^2$.
Let $gcd(a, b) = d,\ d \in \mathbb{Z}$.
Case 1: a, b are relatively prime, i.e, $d = 1$:
If $a^2 + b^2 = N$ with a, b relatively prime then we showed earlier that N can only be divisible by 2 or primes of the form $p \equiv 1 \pmod 4$.
Now $2 = (1 + i)(1 - i)$ and any $p \equiv 1 \pmod 4$ is factored as $p = (u + iv)(u - iv)$. $1 + i, 1 - i, u + iv, u - iv$ are all prime Gaussian integers because their norm is prime.

The nature of primes in Gaussian integers -page 3

Let $s + it$ be one of the above factors, a factor of one the primes dividing N. Then $s + it$ divides $\alpha\overline{\alpha}$.

Since all of these are prime elements (because their norm is a prime – either 2 or $p \equiv 1 \pmod 4$), it means they divide either α or $\overline{\alpha}$.

Suppose $s + it$ divides α. Let us say $\alpha = (s + it)\beta$. Then β has to be a unit and we are in one of the cases above, more precisely either a unit times $1 + i$ or $1 - i$ or a unit times $u + iv$ such that $N(u + iv) = p \equiv 1 \pmod 4$.

If it divides $\overline{\alpha}$ then by taking conjugates we get back to one of the cases above.

The nature of primes in Gaussian integers - page 4

Case 2: $gcd(a, b) = d,\ d > 1$.

In this case $\alpha = d(e + if)$ for some integers e, f.
Since $d > 1$ this means that $e + if$ is a unit, or else α won't be a prime element, because d is not a unit.
Then $\alpha = d$ and $N = d^2$.
So $\alpha = d$ is prime as a rational integer. Each divisor of d has to be congruent to 3 mod 4 because otherwise it would be divisible by some $p = (u + iv)(u - iv)$ with each factor not a unit and hence d won't be a prime. But because it is prime, there can only be one prime divisor congruent to 3 mod 4 and so d must be a prime congruent to 3 mod 4, times a unit (possibly).

Number of ways to write as sum of two squares – Legendre's theorem

Theorem:
Number of ways to write N as $a^2 + b^2$ *equals* $4(D_1 - D_3)$.

D_1 is number of divisors that are 1 mod 4, D_3 is number of divisors 3 mod 4.

$$\textit{Earlier}: \quad N = a^2 + b^2 \implies N = 2^m p_1^{e_1} p_2^{e_2} \ldots . p_k^{e_k} M^2$$

where p_i are 1 mod 4 and M is composed of primes 3 mod 4.

Breaking down the p_i into sums of squares, and
$2 = (1+i)(1-i) = (1+i)^2(-i)$

$$N = (1+i)^{2m}(-i)^m(a_1+b_1 i)(a_1-b_1 i)^{e_1} \ldots . (a_k+b_k i)^{e_k}(a_k-b_k i)^{e_k} M^2$$

We will figure out number of ways to write as sum of squares using this.

Legendre's theorem on sums of squares -page 2

We had:

$$N = (1+i)^{2m}(-i)^m(a_1+b_1 i)(a_1-b_1 i)^{e_1}.....(a_k+b_k i)^{e_k}(a_k-b_k i)^{e_k} M^2$$

Key point
Number of ways to write N as $a^2 + b^2$
= Number of ways to write N as $(a + bi)(a - bi)$.

This in turn depends mainly on number of ways to choose one factor from each pair $(a_k + b_k i)(a_k - b_k i)$. (See page 5 for how M and $(1 + i)^{2m}$ don't affect the count).

Legendre's theorem on sums of squares -page 3

Number of ways to choose one factor from each pair $(a_k + b_k i)(a_k - b_k i)$ is $(e_1 + 1)(e_2 + 1)....(e_k + 1)$.
(Note that $(a + bi)(a - bi) = a^2 + b^2$ while $(a - bi)(a + bi) = a^2 + (-b)^2$ in this theorem).

For each of those versions $N = a^2 + b^2 = (a + bi)(a - bi)$ we get 4 ways to rewrite the sum as $(-a)^2 + b^2, a^2 + (-b)^2$ etc by multiplying by the units $1, -1, i, -i$.

So total number of ways equals $4(e_1 + 1)(e_2 + 1)....(e_k + 1)$.

CLAIM: $(e_1 + 1)(e_2 + 1)....(e_k + 1) = D_1 - D_3$.

Legendre's theorem on sums of squares -page 4

Want to show: $(e_1 + 1)(e_2 + 1)....(e_k + 1) = D_1 - D_3$ where $N = 2^m p_1^{e_1} p_2^{e_2} ....p_k^{e_k} M^2$

Easy to see: Number of divisors constructed from $p_1^{e_1} p_2^{e_2} ....p_k^{e_k}$ is $(e_1 + 1)(e_2 + 1)....(e_k + 1)$. All of these will be 1 mod 4.

But we will also get some divisors that are 1 mod 4 by multiplying any two divisors that are 3 mod 4 because $3^2 \equiv 1 \pmod 4$. You can also get divisors 1 mod 4 by mutliplying two divisors that are 3 mod 4 with a divisor that is 1 mod 4. Basically it turns out that D_3 equals the number of divisors in D_1 that have products of both kinds of divisors. Please read textbook for the proof of that.

In next slide we look at the remaining possibilities.

Legendre's theorem on sums of squares -page 5

What about M^2 and $(1+i)^{2m}$?

These two factors don't contribute anything.
Firstly, as we have seen earlier, if a prime that is 3 mod 4 divides (a+bi)(a-bi) then it HAS to divide one of them because it is a Gaussian prime as well.

But once it divides a+bi or a-bi, it has to divide both a and b, because if any integer divides a Gaussian integer, it has to divide both real and imaginary parts.

So every $a+bi$ we choose would be of form $M(c+di)$ and so M does not give any new ways to choose $a+bi$.

Legendre's theorem on sums of squares -page 6

As for $(1+i)^{2m}$ the same reasoning applies:

In any product $a+bi$ times $a-bi$ each factor must be a multiple of $(1+i)^m$ because otherwise the conjugate would have different norm.

So all the choice happens among the factors of the p_i, as we claimed earlier.