

1.1, 1.3

Nothing too interesting

1.4 Infinite Descent

Did this in number theory
relatively simple example

1.5 Fermat's in Degree 4

$$a^2 + b^2 = c^2$$

exists relatively prime q and p where $p > q$ where if a even then $a = 2pq$, $b = p^2 - q^2$, $c = p^2 + q^2$

Theorem: area of a pythagorean triangle can't be square (descent argument)

Corollary: Fermat holds for $n = 4$. Also, in an exercises they have $x^4 + y^4 = 2z^4$ and $x^4 + y^4 = 2z^2$

Fermat was interested in looking at forms of type $X^2 + AX^2$ where $A \in \{1, 2, 3\}$

1.6. Theorem of two squares

Theorem 1.6.1 (Theorem of two squares): $n = x^2 + y^2$ iff all prime factors of n of form $4m - 1$ have even exponents

Look at $\mathbb{Z}[i]$, define norm to be $N(x + iy) = x^2 + y^2$: this is a homomorphism from $\mathbb{Z}[i] \setminus \{0\} \rightarrow \mathbb{N}^*$

$\mathbb{Z}[i]$ is now a Euclidean ring, and since it's principal, anything in $\mathbb{Z}[i]$ can be written as $u\pi_1^{n_1} \dots \pi_r^{n_r}$ where each π_i is irreducible and $N(u) = 1$

Let U be the kernel of N and Σ be its image; that is $U = \{x \in \mathbb{Z}[x] : N(x) = 1\}$ and $\Sigma = \{n \in \mathbb{Z} : N(x) = n \exists x \in \mathbb{Z}[x]\}$

Theorem 1.6.2 If $p \in \mathbb{N}^*$ is prime then the following are equivalent:

- (a) $p \in \Sigma$
- (b) p is reducible in $\mathbb{Z}[i]$
- (c) $p = 2$ or $p \equiv 1 \pmod{4}$

Proof. If $p \in \Sigma$ then $p = (a + bi)(a - bi)$, so (i) \rightarrow (ii).

If $p = z_1 z_2$ with $z_1, z_2 \notin U$ then $N(p) = N(z_1)N(z_2)$ (because N is a homomorphism), so $p^2 = N(z_1)N(z_2)$. But since $N(z_1) > 1$ and $N(z_2) > 1$ we have $p = N(z_1) = N(z_2)$ so $p \in \Sigma$.

For (ii) \Leftrightarrow (iii), look at pg 11. Also, ask how (p) reducible iff $X^2 + 1$ factors in $\mathbb{F}_p[x]$

Euler's criterion: if p is an odd prime and a is a positive integer such that $p \nmid a$, then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$

where $\left(\frac{a}{p}\right)$ is 0 if $p \mid a$, 1 if a is a quadratic residue modulo p , -1 if a is a nonquadratic residue of p

quadratic residue means there's an x such that $x^2 \equiv a \pmod{p}$

quadratic nonresidue means there's isn't an x

From this, **proof of theorem of two squares:**

If $n = n_1 n_2$ where n_1 has the prime factors in Σ and n_2 has the factors that aren't, then $n_1 \in \Sigma$ since Σ is a monoid (so closed). If n_2 is square, then $n \in \Sigma$. If $n \in \Sigma$ and n_2 isn't square then there is a contradiction as follows:

Let $n = a^2 + b^2$. If $q = -1 \pmod{4}$ is prime, $q \mid a$ and $q \mid b$ then $q^2 \mid n$. Can do the same thing for $n \mid q^2$ which means the none of the common divisors of a and b are congruent to $-1 \pmod{4}$.

If n_2 isn't square then it has a prime factor q congruent to $-1 \pmod{4}$ whose exponent is odd.

Thus q doesn't disappear in the reduction above, so we just have the case $a^2 + b^2 \equiv 0 \pmod{q}$ with $a \not\equiv 0$ and $b \not\equiv 0$.

This means $ab \not\equiv 0 \pmod{q}$, and when we divide by b we get

$$\left(\frac{a}{b}\right)^2 + 1 \equiv 0 \pmod{q}.$$

But $q \not\equiv 1 \pmod{4}$, so we have a contradiction (why?)

There's also a more classical "Fermat" style proof that doesn't use modern algebra

Representations as sums of two squares

Define $r(n)$ as the number of ways n can be written as $a^2 + b^2$, all distinct even if they're just sign changes or variable swaps

Theorem 1.6.4 Let $n \in \mathbb{N}$ and let

$$n = 2^\alpha \prod p^{v_p(n)} \prod q^{v_q(n)}$$

where p 's and q 's are the primes congruent to 1 and -1 mod 4. Then:

- $r(n) = 0$ if all the $v_q(n)$ aren't even
- $r(n) = 4 \prod p^{v_p(n)+1}$ if they are all even

(proof is an exercise)

couple other lemmas, trying to lead to Euler's proof for $n = 3$, using $\mathbb{Z}[\sqrt{-3}]$