

Overview:

- basic arithmetic
- quadratic reciprocity and quadratic forms:

SAMPLE THRM: Given positive integer n , it can be written as $n = x^2 + y^2$ with x, y integers with no common factors iff all prime factors of n are of the form $4k+1$, except for 2 which may occur only once.

ex: $12 = 2^2 \cdot 3$ $85 = 5 \cdot 17 \checkmark$, $85 = 49 + 36 = 81 + 4$

- Pell's equation

$x^2 - dy^2 = N$, where d, N integers (fixed), d square free

SAMPLE THRM: $N=1$ thrm $x^2 - dy^2 = 1$.

There exists a solution (x_1, y_1) s.t. all other solns are (x_n, y_n) $n=1, 2, 3, \dots$ with $x_n + y_n \sqrt{d} = (x_1 + y_1 \sqrt{d})^n$

(x_2, y_2) $(x_1 + y_1 \sqrt{d})^2 = x_1^2 + 2x_1 y_1 \sqrt{d} + y_1^2 d$

$\therefore (x_1^2 + y_1^2 d, 2x_1 y_1 \sqrt{d}) = (x_2, y_2)$

- elliptic curve
 - state Theorem of Faltings
- (these topics are "hopefuls")

} $f(x, y)$ poly. with integer coeff.

understand solns of $f(x, y) = 0$

Divisibility:

Def: An integer b is divisible by an integer a iff \exists integer c s.t. $b = a \cdot c$

Notation: b div. by a : $a|b$

b not div by a : $a \nmid b$

Properties:

- 1) $a|b \Rightarrow a|bc \quad \forall$ integers c
- 2) $a|b, b|c \Rightarrow a|c$
- 3) $a|b, a|c \Rightarrow a|(bx+cy) \quad \forall x, y \in \mathbb{Z}$
- 4) $a|b, b|a \Rightarrow a = \pm b$
- 5) $a|b, a > 0, b > 0 \Rightarrow a \leq b$
- 6) if $n \neq 0$, then $a|b$ iff $na|nb \quad (n \in \mathbb{Z})$

Proof as homework.

Thm: (Division algorithm):

Given $a, b \in \mathbb{Z}$, $a > 0$. Then $\exists! q, r \in \mathbb{Z}$ s.t.

$b = qa + r$ and $0 \leq r < a$. If $a \nmid b$, then $r \neq 0$

Proof:

Existence:

consider $\dots, b-2a, b-a, b, b+a, b+2a, \dots$

increasing seq. tends to $-\infty$ to left & ∞ to right.

Let $r =$ smallest non-neg. elt. in seq.

$\therefore r = b - qa$, for some q .

$$b = qa + r.$$

By assumption, $0 \leq r$

If $r \geq a$, $b - (q+1)a \geq 0$, which contradicts minimality of r

Uniqueness: Suppose $b = qa + r$ and $b = q'a + r'$

$$0 = b - b = (q - q')a + (r - r')$$

$$r' - r = (q - q')a$$

$$0 \leq r, r' < a \Rightarrow |r - r'| < a$$

$\therefore a \mid (r' - r)$, contradicts Prop. 5, if $r' - r \neq 0$

Since $a \neq 0$, $q - q' = 0$ as well.

$a \nmid b \Rightarrow r \neq 0$.

$$b = qa + r.$$

Equivalently, $r = 0 \Rightarrow a \mid b$.

If $r = 0$, $b = qa$, so by def. $a \mid b$

ex: Find q, r for $b = 1243$, $a = 372$

$$q = 3 \quad 372 \times 3 = 1116 \quad r = 127$$

$$b = qa + r \Rightarrow \frac{b}{a} = q + \frac{r}{a} \quad 0 \leq \frac{r}{a} < 1$$

Def. An integer a is a common divisor of b and c if $a \mid b$ and $a \mid c$.

$\cdot 1$ is common divisor for any b, c , and the set of common div. is bnded by $|a| \leq \min(|b|, |c|)$.

\therefore The greatest common divisor of b, c exists.

Notation: $\gcd(b, c)$ (b, c)