Number Theory

Jan Nekovář, UPMC, 2016

Books: D.E.FLATH, Introduction to Number Theory, Wiley, 1989
K.IRELAND, M.ROSEN, A Classical Introduction to Modern Number Theory, Springer, 1982
Z.I.BOREVIČ, I.R.ŠAFAREVIČ, Number Theory, Academic Press, 1966
D.A.COX, Primes of the form x^2+ny^2, Wiley, 1989
J-ESMONDE, M.RAM MURTY, Problems in Algebraic Number Theory, Springer, 1999

Principal motivation: study of Diophantine equations

(polynomial equations with coefficients in $\mathbb{Z}$, to be solved in $\mathbb{Z}$ or $\mathbb{Q}$)

Ex: $y^2+11=x^2$ $(x,y\in\mathbb{Z})$ $(x,y)=(3,\pm 4)$, ... ??other solutions??

Ex: $x^2+y^2=3z^2$ $(x,y\in\mathbb{Z})$ use congruences (mod 3)

$x\equiv 0,\pm 1\ (3) \Rightarrow x^2\equiv 0^2,(\pm 1)^2\equiv 0,1\ (3)$
$y^2\equiv 0,1\ (3)$
$\Rightarrow 0\equiv 3z^2\equiv \begin{cases}0+0\\0+1\\1+0\\1+1\end{cases}$ (mod 3)

$\Rightarrow 3\mid x,\ 3\mid y \Rightarrow 3\mid z$: $x=3x_1$, $y=3y_1$, $z=3z_1$, $x_1^2+y_1^2=3z_1^2$. Repeat:
get $\forall n\geq 1$ $3^n\mid x$, $3^n\mid y$, $3^n\mid z \Rightarrow$ $x=y=z=0$.

Ex: Fermat's equation $x^n+y^n=z^n$ $(n>2)$ $(x,y,z\in\mathbb{Z})$

Thm (Wiles, 1995) If $x^n+y^n=z^n$ $(x,y,z\in\mathbb{Z})$, $n>2 \Rightarrow xyz=0$.

Note: [$n>2 \Rightarrow 4\mid n$ or $\exists$ prime $p>2$ $p\mid n$] $\Rightarrow$ enough to treat $n=4$ (Fermat), $n=p>2$ prime

Prop. p prime, $x,y\in\mathbb{Z}$, $n\geq 1$, $\boxed{x\equiv y\ (\mathrm{mod}\ p^n) \Rightarrow x^p\equiv y^p\ (\mathrm{mod}\ p^{n+1})}$

Proof. $x=y+p^n z$ $(z\in\mathbb{Z})$, $x^p=y^p+\binom{p}{1}y^{p-1}(p^n z)+\cdots+\binom{p}{p-1}y(p^n z)^{p-1}+(p^n z)^p$

$\binom{p}{1}$ divisible by p; $\binom{p}{p-1}$ divisible by p^n; $(p^n z)^p$ divisible by p^{n+1}.

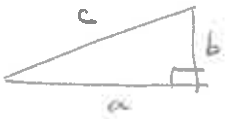
Corollary: (1) $3\nmid x \Rightarrow x\equiv\pm 1\ (3) \Rightarrow x^3\equiv(\pm 1)^3\equiv\pm 1\ (\mathrm{mod}\ 3^2)$
$\pm 1\pm 1\not\equiv\pm 1\ (\mathrm{mod}\ 3^2)$, so $\boxed{x^3+y^3\equiv z^3\ (\mathrm{mod}\ 3^2) \Rightarrow 3\mid xyz}$

(2) $5\nmid x \Rightarrow x\equiv\pm 1,\pm 2\ (\mathrm{mod}\ 5) \Rightarrow x^5\equiv(\pm 1)^5,(\pm 2)^5\equiv\pm 1,\pm 7\ (\mathrm{mod}\ 5^2)$
$\left\{\begin{matrix}\pm 1\\\pm 7\end{matrix}\right\}+\left\{\begin{matrix}\pm 1\\\pm 7\end{matrix}\right\}\not\equiv\left\{\begin{matrix}\pm 1\\\pm 7\end{matrix}\right\}\ (\mathrm{mod}\ 5^2)$, so $\boxed{x^5+y^5\equiv z^5\ (\mathrm{mod}\ 5^2) \Rightarrow 5\mid xyz}$

---

this does not work for $p=7$: $1^7+2^7\equiv 3^7\ (\mathrm{mod}\ 7^2)$

the equation $a^2+b^2=c^2$ $(a,b,c\in\mathbb{Z}_{>0})$



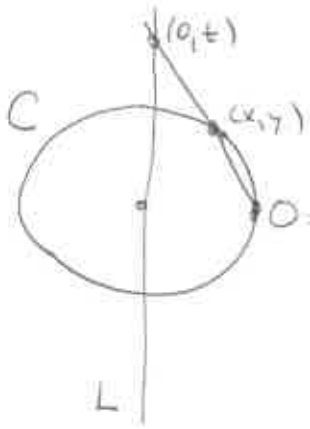
solutions $(3,4,5)$, $(6,8,10)$, $(9,12,15)$, ...
$(5,12,13)$, ... , $(15,8,17)$, ...

4 methods of solution

1st method – geometry ("circle = line")

$\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$

$x^2+y^2=1$ $(x,y\in\mathbb{Q})$



$C: x^2+y^2=1$ circle

$L: x=0$ vertical line

$O=(1,0)\in C(\mathbb{Q})$ rational point of C

central projection (centre $=O$) of C onto L:

$$C(\mathbb{R})\smallsetminus\{O\} \overset{\text{bijection}}{\longleftrightarrow} L(\mathbb{R})\ (\simeq\mathbb{R})$$

$$(x,y) \longmapsto (0,t)\ (\mapsto t)$$

$$\left(\frac{t^2-1}{t^2+1},\frac{2t}{t^2+1}\right) \longmapsto (0,t)\ (\mapsto t) \qquad (*)$$

Computation: $(0,t)$, (x,y), $(1,0)$ are on a line $(x\neq 1)$

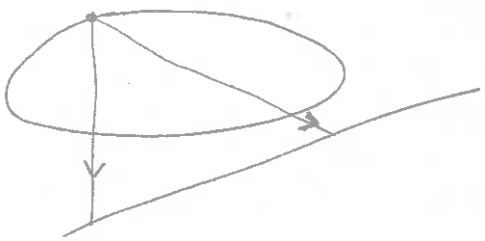
$$0=\begin{vmatrix} 0 & t & 1\\ x & y & 1\\ 1 & 0 & 1\end{vmatrix} = t(1-x)-y,\quad t=\frac{y}{1-x}\ \left(=\frac{1+x}{y}\ \text{if } y\neq 0\right)$$

if $y\neq 0$, $\frac{1}{t}=\frac{1-x}{y}$, $y\left(t+\frac{1}{t}\right)=2$, $y\left(t-\frac{1}{t}\right)=2x$, $x=\frac{t^2-1}{t^2+1}$, $y=\frac{2t}{t^2+1}$

the formulas $(*)$ preserve rationality: $x,y\in\mathbb{Q}\iff t\in\mathbb{Q}$, so we get

$$\begin{array}{ccc} C(\mathbb{Q})\smallsetminus\{O\} & \overset{\text{bijection}}{\longleftrightarrow} & \mathbb{Q}\\ \downarrow & & \downarrow\\ (x,y) & \longleftrightarrow & t\end{array}$$

Questions: (1) What if we replace C by a general conic (ellipse, hyperbole, ...)?



(2) What if we replace $C\subset\mathbb{R}^2$ by a quadric $\{Q(x_1,\dots,x_n)=0\}\subset\mathbb{R}^n$?
What are the solutions of $x_1^2+\dots+x_n^2=1$ $(x_i\in\mathbb{Q})$?

(3) What do the complex solutions $C(\mathbb{C})$ of $x^2+y^2=1$ look like?

2nd method – elementary arithmetic (unique factorisation in $\mathbb{Z}_{>0}$)

Def. A solution of $a^2+b^2=c^2$ $(a,b,c\in\mathbb{Z}_{>0})$ is *primitive* if $\gcd(a,b)=1$

Note: (1) if $a^2+b^2=c^2$ and $d=\gcd(a,b)$, then $d\mid c$ and $\left(\frac{a}{d},\frac{b}{d},\frac{c}{d}\right)$ is a primitive solution

(2) (a,b,c) primitive solution $\Rightarrow \gcd(a,c)=1=\gcd(b,c)$

(3) $a\equiv 0,1 \pmod 2 \Rightarrow a^2\equiv 0,1 \pmod 4$; idem for $b^2, c^2\equiv 0,1 \pmod 4$.

So: $a^2+b^2=c^2 \Rightarrow$ $0+0\equiv 0$, $0+1\equiv 1$, $1+0\equiv 1 \pmod 4$ ← not primitive

Conclusion: (a,b,c) primitive $\Rightarrow$ ($2\nmid a$ and $2\mid b$) or ($2\mid a$ and $2\nmid b$)

After exchanging $a\leftrightarrow b$, we can assume that ↑

Finding primitive solutions with $2\nmid a$, $2\mid b$:

$a^2=c^2-b^2=(c+b)(c-b)$, $c\pm b>0$, $d=\gcd(c+b,c-b)$

what is $d=?$ $\quad d\mid a^2 \Rightarrow 2\nmid d$

$d\mid c+b\pm(c-b) \Rightarrow d\mid \underbrace{\gcd(2c,2b)}_{2\gcd(c,b)=2}$ $\Rightarrow d=1$.

unique factorisation in $\mathbb{Z}_{>0}$: if $a^2=x_1x_2$, $\gcd(x_1,x_2)=1 \Rightarrow x_1=a_1^2, x_2=a_2^2$

So: $c+b=a_1^2$, $c-b=a_2^2$, $a=a_1a_2$, $a_i\in\mathbb{Z}_{>0}$.

$\Rightarrow c=\frac{a_1^2+a_2^2}{2}$, $b=\frac{a_1^2-a_2^2}{2}$. But $2\nmid a \Rightarrow 2\nmid a_1,a_2 \Rightarrow u=\frac{a_1+a_2}{2}$, $v=\frac{a_1-a_2}{2}$

$a_1=u+v$, $a_2=u-v$; $u,v\in\mathbb{Z}_{>0}$

$a=a_1a_2=u^2-v^2$ $b=2uv$ $c=u^2+v^2$	$u,v\in\mathbb{Z}_{>0}$, $u>v$, $u\not\equiv v \pmod 2$ $\gcd(u,v)=1$

Note: $a+bi=(u+vi)^2$, $c=(u+vi)(u-vi)$, $z\bar z=1$

$z=x+iy=\frac{a+bi}{c}=\frac{u+vi}{u-vi}$

$(2+i)^2=3+4i$
$(3+2i)^2=5+12i$
$(4+i)^2=15+8i$

Complex reformulation: $z=e^{i\theta}$

$w=re^{i\theta/2}$, $r\in\mathbb{R}-\{0\}$

$$\{z\in\mathbb{C}\mid z\bar z=1\}=U(1)=\left\{\frac{w}{\bar w}\;\middle|\; w\in\mathbb{C}-\{0\}\right\}$$

We have proved the same result "with rational coefficients":

$$\left\{z=x+iy\;\middle|\; x,y\in\mathbb{Q},\ z\bar z=1\right\}=\left\{\frac{w}{\bar w}\;\middle|\; w=u+vi\neq 0,\ u,v\in\mathbb{Q}\right\} \quad (*)$$

We now prove an abstract version of this.

3rd method – algebra: complex conjugation $\mathbb{C} \longrightarrow \mathbb{C}$, $\overline{z_1+z_2} = \overline{z_1}+\overline{z_2}$, $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$, $\overline{1}=1$, $\overline{\overline{z}} = z$

Abstract situation: • L = field (e.g. $L=\mathbb{C}$)

• $\sigma: L \longrightarrow L$ a field morphism (e.g. $\sigma(z) = \overline{z}$):

$\sigma(x+y) = \sigma(x)+\sigma(y)$, $\sigma(xy) = \sigma(x)\sigma(y)$, $\sigma(1)=1$ ($\Rightarrow \sigma(0)=0$),

if $x \neq 0$ $\quad 1 = \sigma(x \cdot \frac{1}{x}) = \sigma(x)\sigma(\frac{1}{x}) \Rightarrow \sigma(\frac{1}{x}) = \frac{1}{\sigma(x)}$, $\sigma(x) \neq 0$; so σ is injective

• $\sigma \neq id$ $\quad (\exists\, x \in L \quad \sigma(x) \neq x)$

• σ = involution, $\sigma^2 = id$: $\forall x \in L \quad \sigma(\sigma(x)) = x$

Then: $K = L^{\sigma=id} = \{ x \in L \mid \sigma(x) = x \}$ is a subfield of L (e.g. $K = \mathbb{R}$)

Thm (Special case of Hilbert's Theorem 90)

$$\{ \alpha \in L \mid \underbrace{\alpha \cdot \sigma(\alpha)}_{N_{L/K}(\alpha)} = 1 \} = \{ \frac{\beta}{\sigma(\beta)} \mid \beta \in L \setminus \{0\} \}$$

(the norm)

Our case: $L = \mathbb{Q}(i)$ (= the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}, i$)

$= \{ x+iy \mid x, y \in \mathbb{Q} \}$

This is a field: stable under $+, \cdot$; contains 1

$0 \neq z = x+iy \in L \Longrightarrow \frac{1}{z} = \frac{x-iy}{x^2+y^2} \neq 0 \in L$.

$\sigma: L \longrightarrow L$, $\sigma(x+iy) = \overline{x+iy} = x-iy$

$K = L \cap \mathbb{R} = \mathbb{Q}$

Thm gives (*) from the previous page.

Pf of Thm. (2) If $\alpha = \frac{\beta}{\sigma(\beta)} \Rightarrow \sigma(\alpha) = \frac{\sigma(\beta)}{\sigma(\sigma(\beta))} = \frac{\sigma(\beta)}{\beta} = \frac{1}{\alpha} \Rightarrow \alpha\sigma(\alpha) = 1$.

(1) (let $\alpha\sigma(\alpha)=1$) Take any $\gamma \in L$ and look at $\beta = \gamma + \alpha\sigma(\gamma) \in L$:

$\sigma(\beta) = \sigma(\gamma) + \sigma(\alpha)\sigma(\sigma(\gamma)) = \sigma(\gamma) + \frac{1}{\alpha}\gamma \Rightarrow \alpha\sigma(\beta) = \alpha\sigma(\gamma) + \gamma = \beta$

Is $\beta \neq 0$? If $\alpha \neq -1$, take $\gamma = 1$; then $\beta = 1+\alpha \neq 0$.

If $\alpha = -1$, take any $\gamma \in L$, $\gamma \notin K$; then $\beta = \gamma - \sigma(\gamma) \neq 0$.

So $\beta \neq 0$ and $\alpha = \frac{\beta}{\sigma(\beta)}$.

Questions: (1) What does Thm imply about solutions of

$x^2 + 7y^2 = 1$ (or $x^2 - 7y^2 = 1$) $\quad (x, y \in \mathbb{Q})$?

---

(2) What if $\sigma^3 = id$ (or if $\sigma^n = id$)?

4th method – arithmetic of $\mathbb{Z}[i] = \{x+iy \mid x,y\in\mathbb{Z}\}$ (the Gauss integers)

$\boxed{a^2+b^2=(a+bi)(a-bi)=c^2}$

Algebraic terminology: let A be a ring (commutative, with a unit 1)

(1) A is an (integral) domain if $[ab=0 \Rightarrow a=0 \text{ or } b=0]$ $(a,b\in A)$

(2) the multiplicative group of A is $A^*=\{a\in A \mid \exists b\in A\ ab=1\}$ $(b=a^{-1})$
(group with respect to multiplication)

(3) For $a,b\in A$, b divides a (notation: $b\mid a$) if $\exists c\in A\ bc=a$

(4) $\left\{\begin{matrix} a=bu \\ u\in A^*\end{matrix}\right\} \Rightarrow [a\mid b \text{ and } b\mid a]$; the converse "$\Leftarrow$" holds if $A=$ integral domain

(5) $a\in A$ is irreducible if $a\neq 0$, $a\notin A^*$, and $[a=bc \Rightarrow b\in A^* \text{ or } c\in A^*]$

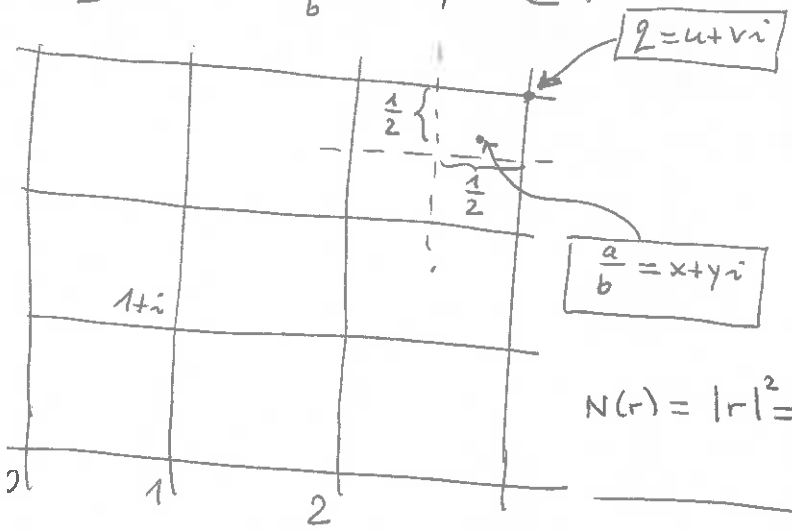
(6) A is a field if $0\neq 1$ and $A^*=A\setminus\{0\}$

(7) A is a Euclidean domain with respect to a function
$\lambda: A\longrightarrow \mathbb{N}=\{0,1,2,\dots\}$ ($\lambda(a)=$ "the size of a") if $A=$domain
and $\forall a,b\in A$, $b\neq 0$ $\exists q,r\in A$ $a=qb+r$, $\lambda(r)<\lambda(b)$
(and $\lambda(a)=0 \Leftrightarrow a=0$)

Proposition. $\mathbb{Z}[i]$ is a Euclidean domain w.r.t. $\lambda(\alpha)=N(\alpha)=\alpha\overline{\alpha}=|\alpha|^2$.

Pf: $\lambda(\underbrace{x+iy}_{\alpha})=x^2+y^2\in\mathbb{N}$, $\lambda(\alpha)=0 \Leftrightarrow x=y=0$.

Given $a,b\in\mathbb{Z}[i]$, $b\neq 0$, let $q=u+vi\in\mathbb{Z}[i]$ be the closest element of the square lattice $\mathbb{Z}[i]=\mathbb{Z}\cdot 1+\mathbb{Z}\cdot i\subset\mathbb{C}$ to the quotient $\frac{a}{b}=x+yi\in\mathbb{C}$:



$u,v\in\mathbb{Z}$

$|x-u|,\ |y-v|\leq\frac{1}{2}$

$\left|\frac{a}{b}-q\right|^2=|x-u|^2+|y-v|^2\leq$

$\leq\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2=\frac{1}{2}<1$

Let $r=a-bq\in\mathbb{Z}[i]$; then

$N(r)=|r|^2=\underbrace{|b|^2}_{N(b)}\underbrace{\left|\frac{a}{b}-q\right|^2}_{<1}<N(b)$.

Prop. $\mathbb{Z}[i]^*=\{\alpha\in\mathbb{Z}[i] \mid N(\alpha)=1\}=\{\pm 1,\pm i\}=\mu_4(\mathbb{C})$

[**Notation**: A ring, $n\geq 1$, $\mu_n(A)=\{a\in A \mid a^n=1\}$]

Pf: if $\alpha,\beta\in\mathbb{Z}[i]$, $1=\alpha\beta \Rightarrow 1=N(1)=N(\alpha\beta)=\alpha\beta\,\overline{\alpha\beta}=\alpha\overline{\alpha}\,\beta\overline{\beta}=N(\alpha)N(\beta)$
$\Rightarrow N(\alpha)=N(\beta)=1$. Conversely, if $N(\alpha)=1=\alpha\overline{\alpha} \Rightarrow \overline{\alpha}=\frac{1}{\alpha}\in\mathbb{Z}[i]$.

Finally, $N(x+iy)=1 \Leftrightarrow x^2+y^2=1$
$\{x,y\in\mathbb{Z} \Rightarrow x=0,\ y=\pm 1 \text{ or } y=0,\ x=\pm 1\}$.

Consequences of the Euclidean property:

- Euclid's algorithm
- the Bézout property: Euclid's algorithm applied to $a, b \in \mathbb{Z}[i] \setminus \{0\}$ terminates and gives $d \in \mathbb{Z}[i] \setminus \{0\}$ such that
  $\underbrace{\mathbb{Z}[i]a + \mathbb{Z}[i]b}_{\{xa+yb \mid x,y \in \mathbb{Z}[i]\}} = \mathbb{Z}[i]d$ — d is unique up to $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$
- $d \mid a$ and $d \mid b$
- if $c \mid a$ and $c \mid b \Rightarrow c \mid d$.

$\Rightarrow$ "$d = \gcd(a,b)$"

Euclid's Lemma: $x, a, b \in \mathbb{Z}[i] \setminus \{0\}$, $x \mid ab$, x irreducible $\Rightarrow x \mid a$ or $x \mid b$

Pf: $d = \gcd(a, x) = ua + vx \mid x$ ($u, v \in \mathbb{Z}[i]$), x irreducible $\Rightarrow d = \begin{cases} x & \overset{d \mid a}{\Rightarrow} x \mid a \\ 1 & \Rightarrow b = b(ua+vx) = \underbrace{uab + bvx}_{\text{divisible by } x} \end{cases}$

up to an element of $\mathbb{Z}[i]^*$

Prop. $\mathbb{Z}[i]$ is a UFD (= unique factorisation domain), namely:

(1) $\forall\, a \in \mathbb{Z}[i] \setminus \{0\}$ $\exists u \in \mathbb{Z}[i]^*$, $\exists\, x_1, \dots, x_r \in \mathbb{Z}[i]$ irreducible ($r \geq 0$) $a = u x_1 \cdots x_r$.

(2) If $u x_1 \cdots x_r = v y_1 \cdots y_s$, $u, v \in \mathbb{Z}[i]^*$, x_i, y_j irreducible $\Rightarrow r = s$ and, after renumbering the x_j's, $\exists\, u_j \in \mathbb{Z}[i]^*$ such that $\forall j$ $x_j = u_j y_j$.

Pf. (1) Induction on $N(a)$: if $N(a) = 1 \Rightarrow a = u \in \mathbb{Z}[i]^*$. Let $N(a) = n > 1$ ($\Rightarrow a \neq 0$, $a \notin \mathbb{Z}[i]^*$). If a = irreducible $\Rightarrow r = 1$, $x_1 = a$. If $a \neq$ irreducible, then $\Rightarrow a = bc$, $b, c \notin \mathbb{Z}[i]^*$. As $N(a) = \underbrace{N(b)}_{>1}\underbrace{N(c)}_{>1} \Rightarrow N(b), N(c) < N(a)$.
Induction hypothesis $\Rightarrow b = u x_1 \cdots x_r$, $c = u' x_1' \cdots x_s'$, $\Rightarrow a = uu' x_1 \cdots x_r x_1' \cdots x_s'$.

(2) If $s = 0 \Rightarrow u x_1 \cdots x_r \in \mathbb{Z}[i]^* \Rightarrow r = 0$. Let $s \geq 1$. As $y_1 \mid u x_1 \cdots x_r$, Euclid's Lemma $\Rightarrow \exists j$ $y_1 \mid x_j$. After renumbering, $j = 1$, $x_1 = y_1 u_1 \overset{x_1 \text{ irred.}}{\Rightarrow} u_1 \in \mathbb{Z}[i]^*$.
Divide by $y_1 \Rightarrow (uu_1) x_2 \cdots x_r = v y_2 \cdots y_s$ and continue. We get $r \geq s$, $\forall j = 1, \dots, s$ $x_j = u_j y_j$ and $u u_1 \cdots u_r x_{r+1} \cdots x_s = v \in \mathbb{Z}[i]^* \Rightarrow r = s$.

Remarks: (a) In general, A = Euclidean domain $\Rightarrow A$ is a UFD, but the proof of (1) is more complicated. Our argument relies on the fact that $A = \mathbb{Z}[i]$ is Euclidean w.r.t. $N: A \longrightarrow \mathbb{N}$ satisfying $N(ab) = N(a)N(b)$, $A^* = \{a \in A \mid N(a) = 1\}$

(b) All of the above works for $\mathbb{Z}[i\sqrt{2}] = \{x + iy\sqrt{2} \mid x, y \in \mathbb{Z}\}$ and $N(\alpha) = \alpha\bar{\alpha} = x^2 + 2y^2$ ($\mathbb{Z}[i\sqrt{2}]^* = \{\pm 1\}$), but not for $\mathbb{Z}[i\sqrt{d}]$ with $d \in \mathbb{Z}_{\geq 3}$ (these rings are not UFD)

Consequences of unique factorisation:

If $A = UFD$, choose representatives $\mathcal{P} = \{\pi\}$ of irreducible elements modulo A^*. Then each $a \in A \setminus \{0\}$ can be written uniquely as

$$a = u \prod_{\pi \in \mathcal{P}} \pi^{\nu_\pi(a)}, \quad u \in A^*, \ \nu_\pi(a) \in \mathbb{N}$$

only finitely many exponents $\nu_\pi(a)$ are non-zero.

Ex: $A = \mathbb{Z}$, $A^* = \{\pm 1\}$, $n \in \mathbb{Z}$ is irreducible $\Leftrightarrow n = \pm p$, p prime number, $\mathcal{P} = \{p;\ p \text{ prime number}\}$

If $b = v \prod_{\pi \in \mathcal{P}} \pi^{\nu_\pi(b)}$ $(v, w \in A^*)$

$$\Rightarrow \begin{cases} (a|b) = uv \prod_{\pi \in \mathcal{P}} \pi^{\nu_\pi(a) + \nu_\pi(b)} \\ (ab) = w \prod_{\pi \in \mathcal{P}} \pi^{\nu_\pi(ab)} \end{cases} \Rightarrow \boxed{\forall \pi \in \mathcal{P} \quad \nu_\pi(ab) = \nu_\pi(a) + \nu_\pi(b)}$$

the greatest common divisor:

~~if~~ if $a, b, c \in A \setminus \{0\}$,

- $b \mid a \Leftrightarrow \exists c \quad bc = a \Rightarrow \forall \pi \quad \nu_\pi(a) \left(= \nu_\pi(b) + \nu_\pi(c)\right) \geq \nu_\pi(b)$

$\Leftarrow$

take $c = \prod_{\pi \in \mathcal{P}} \pi^{\nu_\pi(a) - \nu_\pi(b)}$

- if we define $d = \prod_{\pi \in \mathcal{P}} \pi^{\min(\nu_\pi(a), \nu_\pi(b))}$, then
  - $d \mid a$ and $d \mid b$
  - if $c \mid a$ and $c \mid b \Rightarrow \forall \pi \quad \nu_\pi(c) \leq \nu_\pi(a), \nu_\pi(b) \Rightarrow \nu_\pi(c) \leq \nu_\pi(d)$ $\Rightarrow c \mid d$

Up to A^*, d (= $\gcd(a,b)$) does not depend on the choice of $\mathcal{P}$

Prop. If $A = UFD$, $a, b, c \in A \setminus \{0\}$, $a^n = bc$, $\gcd(b,c) = 1$

$\Rightarrow b = u b_1^n$, $c = v c_1^n$, $u, v \in A^*$, $b_1, c_1 \in A \setminus \{0\}$

Pf: $\forall \pi \in \mathcal{P} \quad \nu_\pi(b) + \nu_\pi(c) = \nu_\pi(a^n) = n\, \nu_\pi(a)$ is divisible by n

if $\nu_\pi(b) \neq 0 \Rightarrow \nu_\pi(c) = 0 \Rightarrow n \mid \nu_\pi(b)$ (idem for c).

Back to $\underbrace{a^2 + b^2}_{(a+bi)(a-bi)} = c^2$, $a, b, c \in \mathbb{Z}_{>0}$ primitive, $2 \nmid a$, $2 \mid b$, $2 \nmid c$

Let $d = \gcd(a+bi, a-bi) \in \mathbb{Z}[i] \setminus \{0\}$ (up to $\mathbb{Z}[i]^*$). We have

$d^2 \mid c^2 \Rightarrow d \mid c$, $d \mid (a+bi) \pm (a-bi)$, $d \mid 2a$, $d \mid 2b$ (in $\mathbb{Z}[i]$)

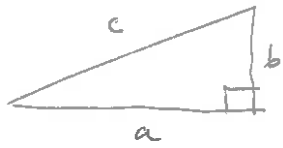
$\Rightarrow N(d) \mid N(c) = c^2$, $N(2a) = 4a^2$, $N(2b) = 4b^2$ (in $\mathbb{Z}$) $\Rightarrow N(d) \mid \gcd(c^2, 4a^2, 4b^2) = 1 \Rightarrow d = 1$

Prop. $\Rightarrow$ $a + bi = \mu \alpha^2$, $\mu = \pm 1, \pm i$, $\alpha = u_1 + v_1 i$, $u_1, v_1 \in \mathbb{Z}$

$a - bi = \overline{\mu}\, \overline{\alpha}^2$ So $a + bi = \mu \underbrace{\left((u_1^2 - v_1^2) + 2u_1 v_1 i\right)}_{2 \nmid a,\ 2 \mid b} \Rightarrow \mu = \pm 1 = \lambda^2$ $(\lambda = 1, i)$

$$\Rightarrow a + bi = (\lambda \alpha)^2 = (u + vi)^2 \qquad u, v \in \mathbb{Z}$$

The problem of congruent numbers



area $\Delta = \frac{ab}{2}$ $\quad$ $a^2+b^2=c^2$

If $(a',b',c') = \lambda(a,b,c)$ $\Rightarrow$ area $\Delta' = \frac{a'b'}{2} = \lambda^2\Delta$

Def: $q \in \mathbb{Q}_{>0}$ is a **congruent number** if $\exists\, a,b,c \in \mathbb{Q}_{>0}$, $a^2+b^2=c^2$, area $= \frac{ab}{2} = q$

(q congruent $\iff$ $\forall \lambda \in \mathbb{Q}_{>0}$ $\lambda^2 q$ congruent)

So it is enough to consider $q = n \in \mathbb{Z}_{>0}$ square-free

Ex: $3^2+4^2=5^2 \Rightarrow \frac{3\cdot 4}{2} = 6$ is a congruent number

$9^2+40^2=41^2 \Rightarrow \frac{9\cdot 40}{2} = 180 = 5\cdot 6^2$ — " — $\Rightarrow$ so is 5

Algebraic formulation: $a^2+b^2=c^2$, $a,b,c \in \mathbb{Q}_{>0} \iff (a,b,c) = c\left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}, 1\right)$, $t \in \mathbb{Q}_{>1}$

$$\Delta = \frac{ab}{2} = \left(\frac{c}{t^2+1}\right)^2 (t^3-t)$$

So: $q \in \mathbb{Q}_{>0}$ is a congruent number $\iff$ $\boxed{\exists\, t,s \in \mathbb{Q},\ t>1,\ qs^2 = t^3-t}$

$\left[\exists\, t,s \in \mathbb{Q},\ s\neq 0,\ qs^2 = t^3-t\right]$ $\overset{\text{exercice}}{\iff}$ $(s/t^2, -1/t) \leftrightarrow (s,t)$

$\iff \exists\, a,b,c \in \mathbb{Z}_{>0}$ primitive solution of $a^2+b^2=c^2$, $\frac{ab}{2} = qs^2$, $s \in \mathbb{Q}$

Conjecture: if $n \in \mathbb{Z}_{>0}$ is square-free and $n \equiv 5,6,7 \pmod 8$ $\Rightarrow$ n is a congruent number (proved if $n=p$ prime, $p \equiv 5,7 \pmod 8$) by Monsky

---

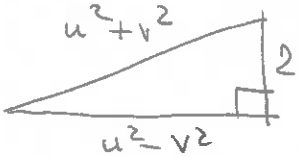
Theorem (Fermat) $1 \neq$ congruent number.

($\iff$ the only solutions of $s^2 = t^3-t$ ($s,t \in \mathbb{Q}$) are $s=0$, $t=0,\pm 1$)

Cor: If $a^2+b^4=c^4$, $a,b,c \in \mathbb{Z} \Rightarrow abc=0$.

Pf: if $b \neq 0 \Rightarrow \left(\frac{ac}{b^3}\right)^2 = \left(\frac{c^2}{b^2}\right)^3 - \frac{c^2}{b^2} \overset{\text{thm}}{\Rightarrow} ac = 0$.

Pf of thm: infinite descent. Assume $\exists$ primitive solution $(a,b,c) = (u^2-v^2, 2uv, u^2+v^2)$ of $a^2+b^2=c^2$ s.t. $\Delta = \frac{ab}{2} = (u^2-v^2)uv$ is a square. We know: $u>v>0$, $u \not\equiv v \pmod 2$, $\gcd(u,v)=1$.



$uv(u+v)(u-v) = w^2$, $w \in \mathbb{Z}_{>0}$

$\gcd(u,v) = \gcd(u, u\pm v) = \gcd(v, u\pm v) = 1$

$2 \nmid d = \gcd(u+v, u-v)$, $d \mid \gcd\left(\underbrace{u+v+(u-v)}_{2u}, \underbrace{u+v-(u-v)}_{2v}\right) = 2$

$\Rightarrow d=1$. So $u, v, u\pm v \in \mathbb{Z}_{>0}$ are pairwise relatively prime, their product is a square $\Rightarrow$ each of them is a square: $u = A^2$, $v = B^2$, $u+v = C^2$, $u-v = D^2$

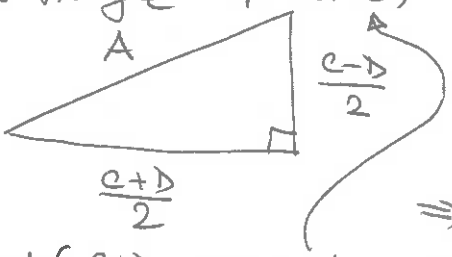
$ABCD = w$ $\quad$ $2 \nmid CD$

So, $u=A^2,\ v=B^2,\ u+v=C^2,\ u-v=D^2,\ w=ABCD$, $2 \nmid CD$

$\Rightarrow C^2, D^2 \equiv 1 \pmod 4 \Rightarrow 2 \nmid u,\ 2 \mid v \Rightarrow 2 \mid B$

$$\left(\frac{C+D}{2}\right)^2+\left(\frac{C-D}{2}\right)^2=\frac{C^2+D^2}{2}=u=A^2$$

new triangle (primitive)



new area $\Delta_1 \overset{\#}{=} \frac{C^2-D^2}{8}=\frac{v}{4}=\left(\frac{B}{2}\right)^2$ again a square!

But $\Delta = w^2$ and $\frac{B}{2} < w$

$\Rightarrow \boxed{0<\Delta_1<\Delta}$

$\gcd\left(\frac{C+D}{2}, \frac{C-D}{2}\right) \mid \gcd\left(A^2, \frac{v}{2}\right)=1$

We can repeat the same procedure with this triangle, etc.:
we obtain triangles with (square) areas

$$\Delta > \Delta_1 > \Delta_2 > \dots > 0,$$ but

$\mathbb{Z}_{>0}$ cannot contain an infinite (strictly) decreasing sequence. Contradiction!

Exercise: (1) $2 \neq$ congruent number

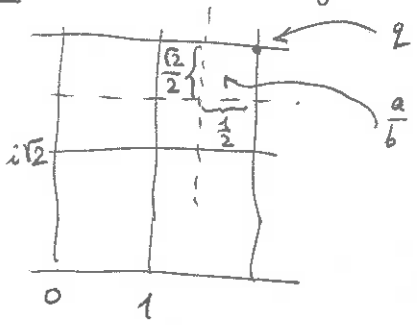
(2) $p \equiv 3 \pmod 8$ prime $\Rightarrow p \neq$ congruent number.

Remark: One can also use descent to prove existence of solutions of certain diophantine equations (see later).

Unique factorisation and diophantine equations

Prop. $\mathbb{Z}[i\sqrt{2}] = \{x+iy\sqrt{2} \mid x,y\in\mathbb{Z}\}$ is a Euclidean domain with respect to $\lambda = N : \mathbb{Z}[i\sqrt{2}] \longrightarrow \mathbb{N}$, $N(\alpha) = \alpha\overline{\alpha} = x^2+2y^2$. Moreover, $\mathbb{Z}[i\sqrt{2}]^* = \{\alpha \mid N(\alpha)=1\} = \{\pm 1\}$.

Pf : the division algorithm works for geometric reasons, as (it does) for $\mathbb{Z}[i]$:



$$\left|\frac{a}{b}-q\right|^2 \le \left(\frac{1}{2}\right)^2+\left(\frac{\sqrt{2}}{2}\right)^2 = \frac{3}{4} < 1 .$$

Corollary : $\mathbb{Z}[i\sqrt{2}]$ is a UFD

(use $N(\alpha\beta)=N(\alpha)N(\beta)$ to prove existence of factorisation into irreducibles, and Euclid's Lemma to prove its uniqueness).

Ex : Solve $y^2+2=x^3$ $(x,y\in\mathbb{Z})$: $\pmod 4 \Rightarrow 2\nmid xy$

$(y+i\sqrt{2})(y-i\sqrt{2})$ $\qquad d = \gcd(y+i\sqrt{2},\ y-i\sqrt{2})$ in $\mathbb{Z}[i\sqrt{2}]$

$d \mid \underbrace{(y+i\sqrt{2})\pm(y-i\sqrt{2})}_{2y,\ 2i\sqrt{2}}$, $d^2 \mid x^3$ in $\mathbb{Z}[i\sqrt{2}] \Rightarrow N(d)^2 \mid \underbrace{\gcd((4y^2)^2, 8^2, x^6)}_{1}$ in $\mathbb{Z}$ $\Rightarrow \boxed{d=1}$

So : $\exists\ \alpha\in\mathbb{Z}[i\sqrt{2}]$, $\exists\ u\in\mathbb{Z}[i\sqrt{2}]^* = \{\pm 1\}$ $(\Rightarrow u=u^3)$ $\quad y+i\sqrt{2} = u\alpha^3 = (u\alpha)^3 = (a+bi\sqrt{2})^3$

$y = a(a^2-6b^2)$, $1 = b(3a^2-2b^2)$ $(a,b\in\mathbb{Z}) \Rightarrow b=\pm 1$, $3a^2 = 2+(\pm 1) \Rightarrow b=1,\ a=\pm 1$

$x^3 = N(a+bi\sqrt{2})^3 \Rightarrow x = a^2+2b^2$ $\qquad \boxed{x=3,\ y=\pm 5}$ $\qquad \boxed{5^2+2=3^3}$

Ex : $\mathbb{Z}[i\sqrt{3}] \neq$ UFD : $2\cdot 2 = (1+i\sqrt{3})(1-i\sqrt{3})$, 2 irreducible, $2\nmid 1\pm i\sqrt{3}$ in $\mathbb{Z}[i\sqrt{3}]$

$\{x+iy\sqrt{3} \mid x,y\in\mathbb{Z}\}$

Better rings : if $\theta = \frac{1+i\sqrt{d}}{2}$, $d\in\mathbb{Z}_{>0}$, $d\equiv 3 \pmod 4 \Rightarrow \theta^2-\theta+\underbrace{\frac{1+d}{4}}_{\in\mathbb{Z}} = 0$

$\Rightarrow \mathbb{Z}\cdot 1+\mathbb{Z}\cdot\theta = \{x+y\theta \mid x,y\in\mathbb{Z}\} \subset \mathbb{C}$ is a ring, equal to

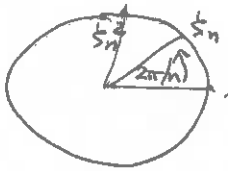
$\mathbb{Z}[\theta]$ = the smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and θ.

$N : \mathbb{Z}[\theta] \longrightarrow \mathbb{N}$, $\quad N(\alpha) = \alpha\overline{\alpha} = (x+y\theta)(x+y\overline{\theta}) = x^2+xy+\frac{1+d}{4}y^2$

$N(\alpha\beta) = N(\alpha)N(\beta)$.

Exercise : (1) $\mathbb{Z}\left[\frac{1+i\sqrt{d}}{2}\right]^* = \{\alpha \mid N(\alpha)=1\} = \begin{cases} \{\pm 1\} & d>3 \\ \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\} = \mu_6(\mathbb{C}) & d=3 \end{cases}$

$\zeta_n = e^{2\pi i/n}$



(2) If $d=3,7,11 \Rightarrow \mathbb{Z}\left[\frac{1+i\sqrt{d}}{2}\right]$ is a Euclidean domain ($\Rightarrow$ UFD) for $\lambda = N$

(3) Solve $y^2+11=x^3$, $x,y\in\mathbb{Z}$ $\quad (y^2+11 = (y+i\sqrt{11})(y-i\sqrt{11}))$

(4) Solve $y^2+y^4+2=x^5$, $x,y\in\mathbb{Z}$ $\quad (y^2+y+2 = (y+\frac{1+i\sqrt{7}}{2})(y+\frac{1-i\sqrt{7}}{2}))$

(5) What happens if you try to solve

$y^2+y+1=x^3$ $\quad (x,y\in\mathbb{Z})$ by the same method ?
