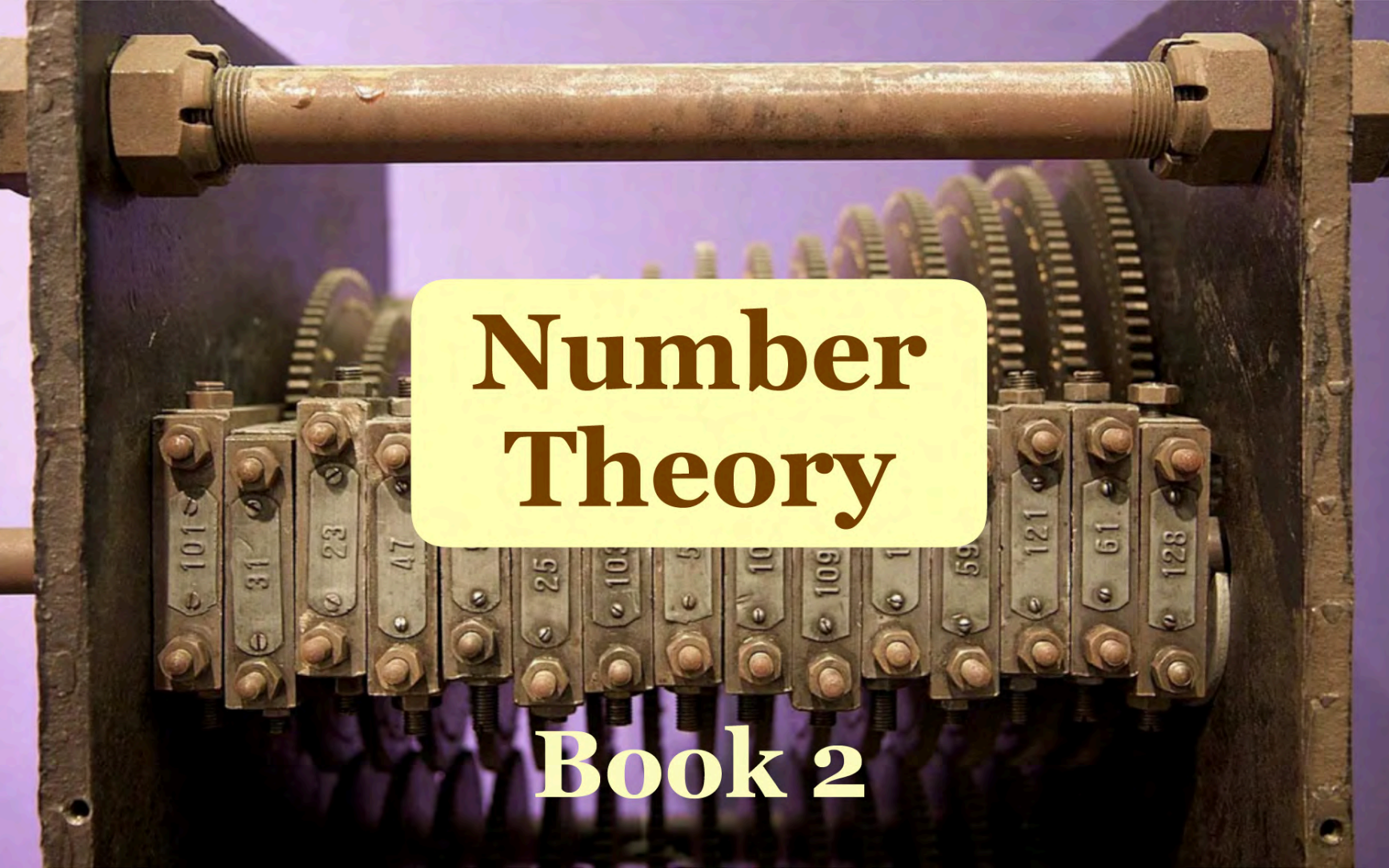
Number
Theory
Book 2

"Trick" (or technique) for identifying which small integers have the form x^2+y^2 or x^2+3y^2 or ...

Define $\theta(t) = \sum_{n=-\infty}^{\infty} t^{n^2} = 1 + 2t + 2t^4 + 2t^9 + 2t^{16} + 2t^{25} + \cdots = \sum_{n\in\mathbb{Z}} t^{n^2}$

$\theta(t)^2 = (1+2t+2t^4+2t^9+2t^{16}+2t^{25}+\cdots)(1+2t+2t^4+2t^9+2t^{16}+2t^{25}+\cdots) = 1 + 4t + 4t^2 + 4t^4 + 8t^5 + 4t^8 + \cdots + 12t^{25} + \cdots$

The powers of t appearing in this expansion are precisely the exponents expressible as a sum of two squares. The coefficient of t^n on the right hand side is the number of solutions of $n = x^2+y^2$ $(x,y\in\mathbb{Z})$

eg. $25 = x^2+y^2$ has 12 solutions $(\pm5, 0)$, $(0,\pm5)$, $(\pm3, \pm4)$, $(\pm4, \pm3)$

$5 = x^2+y^2$ has 8 solutions $(\pm2, \pm1)$, $(\pm1, \pm2)$

$6 = x^2+y^2$ has 0 solutions.

$\theta(t)^3 = 1 + 6t + 12t^2 + 8t^3 + 6t^4 + 24t^5 + 24t^6 + 12t^8 + \cdots$

$1 = x^2+y^2+z^2$ has six solutions $(\pm1, 0, 0)$, $(0,\pm1, 0)$, $(0, 0, \pm1)$

$2 = $ ... twelve $(\pm1, \pm1, 0)$, $(\pm1, 0, \pm1)$, $(0, \pm1, \pm1)$

$7 = x^2+y^2+z^2$ has 0 solutions

$\theta(t)^4$ has positive coefficient of t^n for every positive integer n

Lagrange's Theorem: every positive integer is a sum of four squares

---

Fundamental Theorem of Arithmetic: Every positive integer is uniquely expressible as a product of primes. We'll explain exactly what this says and we'll prove it.

Fundamental Theorem of Calculus

" " " of Linear Algebra

" " " " Algebra

FTA = Fundamental Theorem of Arithmetic:
Positive integers factor uniquely as products of primes.

eg. $12 = 6\times 2 = 2\times 3\times 2$

$12 = 3\times 4 = 3\times 2\times 2$

$12 = (-2)\times(-6) = 2\times 6$

$12 = \boxed{1}\times 12$

Ignore factors of ± 1 in factorization: these are <u>units</u>. (invertible elements). In $\mathbb{Z}$, the only units are ± 1.

eg. $\mathbb{Z}[i] = \{a+bi : a,b\in\mathbb{Z}\}$ (commutative ring with identity 1) we again have unique factorization. The units are $\pm 1, \pm i$.

$i\cdot(-i) = 1$

$1\cdot 1 = 1$

$(-1)(-1) = 1$

$\mathbb{Z}[i]$ = "Gaussian integers"

Elements of R:
- zero
- units
- irreducible
- reducible.

$12 = 2\times 2\times 3 = \underbrace{(1+i)(1-i)(1+i)(1-i)3}_{\text{cannot be factored any further; they are irreducible.}} = (i-1)(-i-1)(1+i)(1-i)3$

$2+i = i(1-2i)$

$10 = 2\times 5 = (1+i)(1-i)(1+2i)(1-2i) = (1+i)(1-i)(2+i)(2-i)$ "migration of units"

($\times i$, $\times(-i)$)

A (commutative ring with identity) has unique factorization if every nonzero element can be factored as a product of irreducible elements and this factorization is essentially unique (i.e. unique up to permutation of factors and migration of units.

Why don't we just say primes and composites instead of irreducible and reducible elements?

In $\mathbb{Z}$:
zero: 0
units: ± 1
irreducible: $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11, \cdots$
reducible: $\pm 4, \pm 6, \pm 8, \pm 9, \pm 10, \pm 12, \cdots$

In $\mathbb{Z}[i]$:
zero: 0
units: $\pm 1, \pm i$
irreducibles: $\pm 1 \pm i = \{1+i, 1-i, -1+i, -1-i\}$
3 actually $3, -3, 3i, -3i$
$\pm 1 \pm 2i, \pm 2 \pm i$
etc.
reducibles: 2 (actually $2, -2, 2i, -2i$)

A nonzero element $\alpha \in R$ is reducible if
$\alpha \neq 0$, $\alpha \neq$ unit and $\alpha = \alpha_1 \alpha_2$ α_1, α_2 not units.
α is irreducible if the only factorizations $\alpha = \alpha_1 \alpha_2$ have either α_1 or α_2 is a unit.
eg. in $\mathbb{Z}[i]$, 3 is irreducible. If $3 = \beta\gamma$, $\beta, \gamma \in \mathbb{Z}[i]$ then either $\beta \in \{\pm 1, \pm i\}$ or $\gamma \in \{\pm 1, \pm i\}$
2 is reducible since $2 = (1+i)(1-i)$, neither $1+i$ nor $1-i$ is a unit.

Eg. the ring $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ does not have unique factorization.
$\mathbb{Z}[\sqrt{6}] = \{a + b\sqrt{6} : a, b \in \mathbb{Z}\}$ . . . . . .
An example of non-unique factorization in $\mathbb{Z}[\sqrt{6}]$: $6 = 2 \times 3 = \sqrt{6} \times \sqrt{6}$
$2, 3, \sqrt{6}$ are irreducible in $\mathbb{Z}[\sqrt{6}]$.
But be careful: $\mathbb{Z}[\sqrt{6}]$ has infinitely many units.
Pell's equation $x^2 - 6y^2 = 1$ has solutions $(\pm 1, 0)$, $(\pm 5, \pm 2)$
$(5 + 2\sqrt{6})(5 - 2\sqrt{6}) = 1$ in $\mathbb{Z}[\sqrt{6}]$
$x^2 - 6y^2 = -1$ has no integer solutions.
(Look at the equation mod 3)

In $\mathbb{Z}[\sqrt{-5}]$, the only units are ± 1.

Unique factorization is not universal.

Difference between $\mathbb{Z}[i]$, $\mathbb{Z}$, $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt{-5}]$, $\mathbb{Z}[\sqrt{6}]$

$\mathbb{Z}[i]$ unique factorization

$\mathbb{Z}[\sqrt{-5}]$ non-unique factorization

$15 = 3\times 5 = (-3)\times(-5)$ in $\mathbb{Z}$

$15 = 3\times(2+i)(2-i)$ in $\mathbb{Z}[i]$

$= 3\times(1+2i)(1-2i)$

$(2-i)i = 1+2i$, $(2+i)(-i) = 1-2i$

migration of units

$15 = 3\times 5 = (3+\sqrt{2})(-5+5\sqrt{2})$ in $\mathbb{Z}[\sqrt{2}]$

$\times(1+\sqrt{2})$ $\times(-1+\sqrt{2})$

$(1+\sqrt{2})(-1+\sqrt{2}) = 1$

Infinitely many units in $\mathbb{Z}[\sqrt{2}]$: $\pm(1+\sqrt{2})^k = \pm 1, \pm 1\pm\sqrt{2}, \pm 3\pm 2\sqrt{2}, \cdots$

$3^2 - 2\cdot 2^2 = (3+2\sqrt{2})(3-2\sqrt{2}) = 1$

$6 = 2\times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

where all factors $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$

If holds in $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$

Not in $\mathbb{Z}[\sqrt{-5}]$ or $\mathbb{Z}[\sqrt{6}]$.

In $\mathbb{Z}[\sqrt{-5}]$ the only units are ± 1. why

If x is a unit $x = a+b\sqrt{-5}$ then

$x\bar{x} = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2 = 1$

But the only integer solutions are $(a,b) = (\pm 1, 0)$.

$2, 3, 1+\sqrt{-5}, 1-\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ are irreducible.

why? If $2 = \alpha\beta$, $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ then

then $4 = |2|^2 = |\alpha|^2|\beta|^2$

$\alpha = a+c\sqrt{-5}$, $\beta = b+d\sqrt{-5}$

$|\alpha|^2 = (a+c\sqrt{-5})(a-c\sqrt{-5}) = a^2+5c^2$ $\quad |\beta|^2 = b^2+5d^2$

$4 = |\alpha|^2|\beta|^2$ where $|\alpha|^2, |\beta|^2 \in \{1,2,3,4,5,\cdots\}$

$1\times 4 \Rightarrow \alpha$ unit

~~2×2~~ $\quad a^2+5c^2 = 2$ has no solution.

$4\times 1 \Rightarrow \beta$ is a unit.

Why does $\mathbb{Z}$ have unique factorization?

It's rather easy to show every integer factors into primes.

$12 = 3 \times 4 = 3 \times 2 \times 2$

There is no infinite decreasing sequence $n_1 > n_2 > n_3 > n_4 > \cdots > 0$ in the positive integers.

The positive integers are well-ordered. (Equivalently, use induction).

Why is the prime factorization of a positive integer n unique?

Can $n = p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s$ where $p_1, p_2, \cdots, p_r, q_1, q_2, \cdots, q_s$ are primes?

We would need to show that every prime on the left (every p_i) occurs also among $q_1, \cdots, q_s$.

Basic step: If p is a prime and $a, b \in \mathbb{Z}$ with $p \mid ab$, then show $p \mid a$ or $p \mid b$.

Euclid's Lemma: If a prime p divides ab in $\mathbb{Z}$, then $p \mid a$ or $p \mid b$.

("or" is inclusive. Eg. $3 \mid 6 \cdot 9 \Rightarrow 3 \mid 6$ or $3 \mid 9$.)

$6 \mid 4 \cdot 9$ but $6 \nmid 4$, $6 \nmid 9$. We really need p to be prime.

$p \mid ab$ says: $pk = ab$ for some k. Can we argue: p is a prime factor on the left so it's a factor on the right so p is a factor in a or in b. No! This is a common fallacy.

Proof of Euclid's lemma: Suppose $p \mid ab$ ie. $pk = ab$ for some k.
Either $p \mid a$ or $p \nmid a$. If $p \mid a$ we're done. Hence we may assume $p \nmid a$.

Then $\gcd(p, a) = 1 = rp + sa$ for some $r, s \in \mathbb{Z}$. ← p not in this list

Divisors of a: $\pm 1, \cdots, \pm a$

Divisors of p: $\pm 1, \pm p$.

$b = rbp + sab$ is divisible by p since both terms rbp and sab are divisible by p. □

If $p \mid abc$ where p is prime then $p \mid a$ or $p \mid b$ or $p \mid c$.

$p \mid abc \Rightarrow p \mid a$ or $p \mid bc$. $\Rightarrow p \mid a$ or $p \mid b$ or $p \mid c$.

This argument extends to any number of factors ie. if $p \mid q_1 q_2 \cdots q_l$ where p is prime then $p \mid q_j$ for some $j \in \{1, 2, \cdots, l\}$. (To formalize this argument, use induction.)

Fundamental Theorem of Arithmetic Every positive integer has a unique factorization as a product of primes.

If $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ where $p_1, p_2, \cdots, p_r, q_1, q_2, \cdots, q_s$ are primes then $p_1 \mid n$ so $p_1 \mid q_j$ for some $j \in \{1, 2, \cdots, s\}$ so $p_1 = q_j$. Cancel this prime factor from both sides and repeat the argument with the remaining prime factors.

On to Chapter 9.

Look at powers in $\mathbb{Z}/7\mathbb{Z} = \mathbb{F}_7 = \{0,1,2,3,4,5,6\} = \{0,\pm1,\pm2,\pm3\}$ eg. $3^2 = 9 = 2$, $\frac{1}{4} = 2$.

$-3 = 6+6+6 = 4$

x	x^0	x^1	x^2	x^3	x^4	x^5	x^6	x^7	x^8
0	1	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	1	2	4	1	2	4	1	2	4
3	1	3	2	6	4	5	1	3	2
$-3=4$	1	4	2	1	4	2	1	4	2
$-2=5$	1	5	4	6	2	3	1	5	4
$-1=6$	1	6	1	6	1	6	1	6	1

$x^5 = x^{-1} = \frac{1}{x}$ if $x \neq 0$

palindromic sequence $1,4,2,2,4,1$

Theorem Let p be prime. Then for all $a \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{0,1,2,\cdots,p-1\}$, $a^p = a$;

furthermore $a^{p-1} = 1$ if $a \neq 0$.

Remark We really do need p to be prime.

"Fermat's Little Theorem"