Überblick Zahlentheorie (Dujella - Reading Course)

I, Induction & Fibonacci numbers

- Peano's axioms
- induction
- binomial theorem $\left[(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right]$
- Cassini's identity $\left[F_{n+1}F_{n-1} - F_n^2 = (-1)^n, \text{pr.: induction over } n\right]$
- Binet's formula $\left[F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}; \text{pr.: induction over } n\right]$
- formula for generalized Fibonacci numbers $\left[H_1 = p,\ H_2 = q,\ p,q \in \mathbb{N};\ H_{n+2} = q F_{n+1} + p F_n\right]$ $\left[\text{pr.: induction over } n\right]$

II, Divisibility

- division with remainder theorem (uniqueness & validity) $\left[\text{pr.: } (q'-q)b = r - r'\right]$
- characterization of gcd $\left[\gcd(a,b) = \min_{>0}\{ax+by : x,y \in \mathbb{Z}\}\right]$ $\left[\text{pr.: } \gcd \mid d;\ d \mid \gcd\right]$
- Euclid's (extended) algorithm $\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \ldots\right]$
- fundamental theorem of arithmetic (uniqueness of prime factorisation) [pe
- existence of infinitely many primes [Euclid, ζ] vgl. $\prod_{i\in I} p_i = \prod_{j\in J} p_j = x$; induction über $|I|$
- Props: $\gcd(a,b) = \prod_i p_i^{\min\{\alpha_i,\beta_i\}}$; $\gcd \cdot \operatorname{kgV} = |a \cdot b|$

III, Congruences

- calculating with congruences $\left[ax \equiv ay \pmod m \iff x \equiv y \pmod{\frac{m}{\gcd(a,m)}}\right]$ [pr: directly c.p. $ax \overset{\text{mod } m}{=} ax + km \ldots$]
- residue systems: $(x_1,\ldots,x_n)$ is res.s. $\iff$ $(ax_1,\ldots,ax_n)$ is res. s. [directly out of 1]
- divisibility tests (2, 3, 4, 5, (6), 7, 8, 9, (10), 11, 13, 25, 37) [look at $10^m \bmod n$]
- criterion for solutions of $ax \equiv b \pmod m$ $\left[\gcd(a,m) \mid b\right]$ [then exactly d sol. mod m]
- Chinese remainder theorem $\left[\gcd(m_1,\ldots,m_n) = 1 \Rightarrow \text{unique sol. to } x = a_i \pmod{m_i} \bmod \prod_i m_i\right]$
- Euler-Fermat's theorem $\left[a^{\varphi(m)} \equiv 1 \pmod m\right]$ & Fermat's little theorem [use residue systems]
- properties of φ (Euler's totient function) [multiplicativity; $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$] p prime

pr: $\prod_{p \mid n} (1 + \varphi(p) + \ldots + \varphi(p^{\alpha_p})) = \sum_{d \mid n} \varphi(d) = n$

- Wilson's theorem $[(p-1)! \equiv -1 \pmod p]$ [pr.: directly through uniqueness of inverse mod p]
- existence of solutions to $x^2 \equiv -1 \pmod p$ [solutions $\Leftrightarrow p = 2 \vee p \equiv 1 \pmod 4$] [ex.: Wilson; non-ex.: Fermat]
- Hensel's lemma $[f(a) \equiv_{p^i} 0 \wedge f'(a) \not\equiv_p 0 \Rightarrow \exists!\, t \in \{0,\dots,p-1\} : f(a + tp^i) \equiv_{p^{i+1}} 0$] [Taylor exp.] f ... polynomial
- # primitive roots mod p $[\varphi(p-1)]$ [obs.: $\sum_{d \mid p-1} \varphi(d) = p-1 = \sum_{d \mid p-1} \gamma(d)$; Lagrange]
- existence of "interesting" primitive root in all moduli p^j $(j \in \mathbb{N})$ [g pr. root mod $p \Rightarrow$ [pr.: binomial th.; $g' = g + pz$; $\gcd(\varphi, t) = 1$] $\Rightarrow \exists x \in \mathbb{Z}$: $g + px$ is pr. root mod p^j $(\forall j \in \mathbb{N})$] [pr.: necess: 2^j; $n = n_1 n_2$]
- existence of primitive roots mod n [$\exists g$ pr. root $\Leftrightarrow n = 1 \vee 2 \vee 4 \vee p^j \vee 2p^j$ for p odd prime]
- discrete logarithm & solutions to $x^n \equiv a \pmod p$ [unique sol. iff $\gcd(n, p-1) = 1$]
- criterion for finite decimal representation of rational numbers [2 & 5 only prime factors of denominator] [pr.: i) $\frac{p}{q} = \frac{\sum a_i 10^i}{10^n}$; ii) $q = 2^\alpha 5^\beta$; $n = \max\{\alpha, \beta\}$]
- form of rationals [$r \in \mathbb{Q} \Leftrightarrow r$ has finite or eventually periodic decimal representation] pr: consider $10^s p \bmod q$ $s \in \mathbb{N}$
- criterion for pure periodicity in decimal repr. of $r \in \mathbb{Q}$ [no prime factors 2 v 5 in PF of q for $r = \frac{p}{q}$]
- length of pre-period in dec. repr. of $r = \frac{p}{q} \in \mathbb{Q}$ [$\max\{\alpha, \beta\}$ with $q = 2^\alpha 5^\beta q_0$]
- Midy's theorem [$q \neq 2 \vee 5$ prime, $\frac{p}{q} = 0, \overline{b_1 \dots b_n}$: $n \in \mathbb{N}_g \Rightarrow \overline{b_1 \dots b_{n/2}} + \overline{b_{n/2+1} \dots b_n} =$
- existence of infinitely many pseudoprimes to a base b [$n = \frac{b^{2p}-1}{b^2-1}$] $p \nmid b^2 - 1 \equiv \underbrace{99\dots9}_{n/2}$ [$\frac{A \cdot 10^s + B}{10^{2s}-1} = \frac{p}{q}$ Fell-interesting]
- Korselt's criterion [n is Carmichael $\Leftrightarrow$ n composite, square-free $\wedge$ $p \mid n \Rightarrow p-1 \mid n-1$]
- n_{2b} - existence of strong psp. to every base [n is a spsp to at most $\frac{n-1}{4}$ bases]
- # solutions to $x^n \equiv \pm 1 \pmod n$ [$\equiv +1$: exactly $s = \prod_i \gcd(m, \varphi(p_i^{\alpha_i}))$ sols for $n = \prod_i p_i^{\alpha_i}$;
  $\equiv -1$ has solutions iff $\nu_2(n) < r := \min\{\nu_2(p_i - 1)\}$
  $\equiv -1$ has exactly s sols iff it has any]
- The Miller - Rabin primality test [probability that n is composite after testing k bases : $\leq \frac{1}{4^k}$]
- Lagrange: f polynomial with $p \nmid a_n \Rightarrow f(x) \equiv_p 0$ has at most $\deg(f) = n$ sol. mod p
  [pr.: induction over $\deg(f) = n$: $f(x) - f(a) = (x-a)\,g(x)$ $\deg(g) = n-1$]

IV, Quadratic residues

- \# quadratic residues mod p $\left[\frac{p-1}{2}\right]$ [pr.: $\left(-\frac{p-1}{2}, \dots, 0, \dots, \frac{p-1}{2}\right)$; $l^2 \equiv_p k^2$ od $l < k < \frac{p-1}{2}$ $\Rightarrow p \mid k^2 - l^2 = (k+l)(k-l)$ ↯]
- Euler's criterion $\left[\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p\right.$ for p odd prime] [kl. Fermat]
- Gauss' lemma (for the Legendre-symbol) [$\gcd(a,p) = 1 \wedge n = \#\{i : ai \pmod p > \frac{p}{2}\}, i < \frac{p-1}{2}$ $\Rightarrow \left(\frac{a}{p}\right) = (-1)^n$]
  [pr.: quetsche ai in $[1, \dots, \frac{p-1}{2}]$, verwende Euler's criterion]
- criterion for $\left(\frac{2}{p}\right)$ $\left[\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}\right.$ [pr. Notation wie in Gauss Lemma, Betrachtung mod 2]
  furthermore: $\gcd(q, 2p) = 1$, $t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor \Rightarrow \left(\frac{q}{p}\right) = (-1)^t$]
- Gauss quadratic reciprocity law $\left[p \neq q \text{ primes} \Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}} = \begin{cases} -1 & p \equiv q \equiv 3 \pmod 4 \\ 1 & \text{sonst} \end{cases}\right]$
  [pr.: cons.: $S = \{(x,y) \mid 1 \le x \le \frac{p-1}{2}, 1 \le y \le \frac{q-1}{2}\}$, split into S_1, S_2 st. $qx \overset{S_2}{\underset{S_1}{>}} py \Rightarrow \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}$; theorem ↑]
- roots in prime modules $\left[p \equiv_4 3 : x = \pm a^{\frac{p+1}{4}}; \; p \equiv_8 5 : x = a^{\frac{p+3}{8}} \vee a^{\frac{p+3}{8}} 2^{\frac{p-1}{4}};\right.$
  [pr.: i) directly ii) $a^{2k+2} \equiv \pm a$]
  $p \equiv_8 1$: Tonelli's algorithm] [d non-q.r.: $a^{(s-i)t} d^{t_i 2^{s-i}} \dots$ $a^t d^{ts} \equiv_p 1 \Rightarrow$ $\Rightarrow x = a^{\frac{t+1}{2}} d^{ts}$]
- criterion a is quadr. res. mod $Q = \prod_i q_i$ $\left[\forall i : \left(\frac{a}{q_i}\right) = 1\right]$
- Gauss quadr. reciprocity law for the Jacobi symbol $\left[P, Q \text{ rel. prime} \Rightarrow \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{Q-1}{2} \cdot \frac{P-1}{2}}\right]$ [Zerlegen, Jsn.-setzen]
- divisibility of Fibonacci numbers $[m, n \neq 2 \in \mathbb{Z}^+ : F_n \mid F_m \Leftrightarrow n \mid m]$ [pr.: $m = n \cdot k$ induction over k: $F_{n(k+1)} = F_{nk-1} F_n + F_{nk} F_{n+1}$ ↯]
- periodicity of Fibonacci numbers mod $m \in \mathbb{N}$ [period $k \le m^2$] [Schubfachprinzip]

V, Quadratic forms

(
- sum of two squares for primes $[\exists x, y \in \mathbb{N} : p = x^2 + y^2 \Leftrightarrow p = 2 \vee p \equiv_4 1]$
- uniqueness of sum of two squares decomposition of prime $p = 4k+1$
)
- criterion for sum-of-two-squares decomposition of an integer n
  $[\exists x, y \in \mathbb{N} : n = x^2 + y^2 \Leftrightarrow \forall p_i$ in the PFZ(n) with $p_i \equiv_4 3 : \alpha_i = 2k$ for $k \in \mathbb{N}]$
- equivalence of pos. definite binary quad. forms to (unique!) reduced form
- finiteness of distinct reduced forms to a given determinant $d \in \mathbb{Z}$

- criterion for representability of n by quad. form of discriminant d
  [n can be repr. by f with $\mathrm{discr}(f) = d \iff x^2 \equiv d \pmod{4n}$ has sols]
- Lagrange's four-square theorem $[\forall n \in \mathbb{N}\ \exists x,y,z,w \in \mathbb{N}: n = x^2+y^2+z^2+w^2]$
- Gauss' & Legendre's three-square theorem $[\exists x,y,z \in \mathbb{N}: n = x^2+y^2+z^2 \iff \nexists m,k \in \mathbb{N}: n = 4^m(8k+7)]$
- criterion for positive definiteness of ternary quadr. form [$\iff a_{11}>0,\ b = a_{11}a_{22} - a_{12}^2 > 0,\ d>0$]
- equivalent class of ternary qu. form with $d=1$ $[x_1^2+x_2^2+x_3^2]$

VI, Arithmetic functions

- exponent of p in $PFZ(n!)$ $\left[p^k \| n! \Rightarrow k = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor\right]$
- if f is multiplicative, $g(n) = \sum_{d \mid n} f(n)$ is multiplicative
- Möbius inversion formula $\left[f: \mathbb{N} \to \mathbb{C},\ F(n) = \sum_{d \mid n} f(n) \Leftrightarrow f(n) = \sum_{d \mid n} \mu(d)\, F\left(\frac{n}{d}\right)\right]$
- ✱ divisors of n: $\tau(n) = \prod_i (\alpha_i + 1)$
- Σ divisors of n: $\sigma(n) = \sum_{d \mid n} d = \prod_i \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$
- $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$
- estimates for arithmetic function $\left[\sum_{n \le x} \tau(n) = x \ln(x) + O(x)\right.$
  $\sum_{n \le x} \sigma(n) = \frac{1}{12}\pi^2 x^2 + O(x \ln(x))$
  $\left.\sum_{n \le x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \ln(x))\right]$
- ✱ square-free pos. integers $\le x$: $Q(x) = \frac{6}{\pi^2} x + O(\sqrt{x})$

VII, Distribution of primes

- Prime Number Theorem: $\lim_{n \to \infty} \frac{\pi(n)}{n/\ln(n)} = 1$
- estimates for $\pi(n)$ $\left[\frac{n}{8\ln(n)} < \pi(n) < \frac{6n}{\ln(n)}\right.$ (for $n \ge 2$); $\ln(n) - \frac{3}{2} \le \frac{n}{\pi(n)} \le \ln(n) - \frac{1}{2}$ (for $n \ge 67$)$]$
- Bertrand-Chebyshev's theorem $[\forall n \in \mathbb{N}\ \exists p \text{ prime}: n < p \le 2n]$
- Mangoldt function and logarithm $\left[\sum_{d \mid n} \Lambda(d) = \ln n\right]$

- Abel's partial summation formula $\left[S(x) := \sum_{n \in x} a_n ;\ f \in C_1([y,x]);\ (a_n)_n \text{ sequence } \in \mathbb{R}\right.$

$$\Rightarrow \sum_{y < n \in x} a_n f(n) = S(x)f(x) - S(y)f(y) - \int_y^x S(u) f'(u)\, du \quad \left.\right]$$

- Euler-Maclaurin summation formula $\left[y < x \in \mathbb{R},\ f \in C_1([y,x]),\ \{z\} = \text{fractional part of } z\right.$

$$\Rightarrow \sum_{y < n \leq x} f(n) = \int_y^x f(u)\, du + \int_y^x \{u\} f'(u)\, dt - f(x)\{x\} + f(y)\{y\} \quad \left.\right]$$

- more estimates for $\pi(n)$:

  i) for $x \geq 2$: $\pi(x) = \frac{\vartheta(x)}{\ln(x)} + O\left(\frac{x}{\ln^2(x)}\right)$

  ii) for $a < \underbrace{\frac{1}{3}\ln(2) + \frac{1}{2}\ln(3)}_{a_0} \approx 0{,}7804 \wedge b > \frac{3}{2} a_0$: $a \frac{x}{\ln(x)} < \pi(x) < b \frac{x}{\ln(x)}$

- formula for Riemann's ξ on $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\}$: $\xi(s) = \prod_{\substack{p \\ \text{prime}}} \left(1 - \frac{1}{p^s}\right)^{-1}$

- Dirichlet's theorem on primes in arithmetic progression

  [$\gcd(k,l) = 1 \Rightarrow$ ∞ primes $p = kn + l$ is infinite]

X. Diophantine equations

- linear Diophantine equation in 2 var. $(ax+by=c)$: $\gcd(a,b) \nmid c \Rightarrow$ no sol., $\gcd(a,b) \mid c \Rightarrow \infty$ sol.

  [ii) $d(a'x+b'y)=c$; i) ex.: $c = k\cdot\gcd = k\cdot(ax_0+by_0)$; ∞: $\frac{a}{d}(x-x_0) = \frac{b}{d}(y_0-y)$]

- linear Diophantine equation in n var. $\left(\sum_{i=1}^{n} a_i x_i = c\right)$: $\gcd(a_1,\dots,a_n) \mid c \Rightarrow \infty$ sol., $\gcd(a_1,\dots,a_n) \nmid c \Rightarrow$ no sol.

  [ii) as above i) induction over n using the above proof]

- Frobenius number of relatively prime numbers: $\gcd(a_1,a_2)=1 \Rightarrow g(a_1,a_2) = a_1a_2 - a_1 - a_2$

  [pr.: oBdA $x \in \{1,\dots,a_2-1\} \Rightarrow y>0 \Rightarrow$ biggest s.t. we need neg. integers is $y=-1$, $x = a_2-1$]

- form of Pythagorean triples for $y \in \mathbb{N}_g$: $x = m^2-n^2$, $y = 2mn$, $z = m^2+n^2$, $\gcd(m,n)=1$, $m \not\equiv_2 n$

  [pr.: $y^2 = z^2 - x^2 = (z+x)(z-x) = (2k)^2$; $k^2 = ab$ mit $z = a+b$, $x = a-b$]

  general form: $\left(d(m^2-n^2)\right)^2 + (2dmn)^2 = \left(d(m^2+n^2)\right)^2$

- $x^4+y^4=z^2$ has no integer solutions

  [pr.: i) show $\gcd(x,y)=1$ by $\nexists$ starting with (x^2,y^2,z), z minimal ii) use form of PT wlog $y \in \mathbb{N}_g \Rightarrow \nexists$ $\overset{\text{minimality}}{\text{of } z}$]

- $x^4+y^2=z^4$ has no integer solutions

  [pr.: $\nexists$ to minimality of hypothesis, i) y even ii) y odd]

- square Diophantine equation in 3 var. $(x^2+y^2+z^2=v^2)$:

  form of solutions: $(a^2+b^2-c^2-d^2)^2 + (2(ad \mp bc))^2 + (2(ac \pm bd))^2 = (a^2+b^2+c^2+d^2)^2$

  [pr.: i) $p \equiv_4 3 \nmid (v+x),(v-x)$ ii) get rid of prime factors $p \equiv_4 3$ in y^2+z^2 iii) induction over # prime factors of x^2+b^2 with $y^2+z^2 = (a^2+b^2)(c^2+d^2)$]

- existence of solution to Pell's equation $(x^2-dy^2=1)$

  [pr.: def. $x = \frac{x_1x_2 - dy_1y_2}{k}$, $y = \frac{x_1y_2 - x_2y_1}{k}$ for $x^2-dy^2=k$ has ∞ sol.; show i) $x,y \in \mathbb{Z}$ ii) $y \neq 0$ iii) $x^2-dy^2=1$]

- Pell's equation has infinitely many solutions, they are of the form $(x_1+\sqrt{d}y_1)^n$ for $x_1+\sqrt{d}y_1$ fundamental s.

  [pr.: i) directly show $(x_1+\sqrt{d}y_1)^n$ are sol. ii) $(s,t) \neq (x_1+\sqrt{d}y_1)^n$: $(x_1+\sqrt{d}y_1)^m < s+\sqrt{d}t < (x_1+\sqrt{d}y_1)^{m+1}$ $\Rightarrow$ smaller sol. than fundamental $\Rightarrow \nexists$]

- recursive form of solution to Pell's equation: $(x_0,y_0)=(1,0)$, (x_1,y_1) fundamental sol.

  $\rightarrow$ $x_{n+2} = 2x_1x_{n+1} - x_n$; $y_{n+2} = 2x_1y_{n+1} - y_n$

  [pr.: direct computation after noting $(x_{n+1}+y_{n+1}\sqrt{d})(x_1+y_1\sqrt{d}) = x_{n+2}+\sqrt{d}y_{n+2}$, $(x_{n+1}+y_{n+1}\sqrt{d})(x_1-y_1\sqrt{d}) = x_n+y_n\sqrt{d}$]

- criterion for fundamental solution: $a+\sqrt{d}b$ sol. of x^2+dy^2 $\wedge$ $a > \frac{1}{2}b^2-1 \Rightarrow a+b\sqrt{d}$ is fund. sol.
- specially, if $\exists u,v \in \mathbb{N}_{>0}$: $d = u(uv^2+2)$, then $1+uv^2+v\sqrt{d}$ is f.s. of $x^2-dy^2=1$

[pr.: $d = \frac{a^2-1}{b} = \frac{x_1^2-1}{y_1^2} \Rightarrow \delta = \delta_1\delta_2 = (x_1b+y_1a)(x_1b-y_1a) \in \mathbb{N} \Rightarrow a \le \frac{b^2}{2}-1$]

- connection solution of $x^2-dy^2=-1$ and $x^2-dy^2=1$: $x_1+y_1\sqrt{d}$ f.s. to $P(-1)$
$\Rightarrow (x_1+y_1\sqrt{d})^2$ f.s. to $P(1)$ $\wedge$ $(x_1+y_1\sqrt{d})^n$ are i) all sol to $P(-1)$ for $n \in \mathbb{N}_u$
ii) all sol to $P(1)$ for $n \in \mathbb{N}_g$

[pr.: i) ξ f f.s. $< (x_1+y_1\sqrt{d})^2$ ii) $(x_1+y_1\sqrt{d})^{2k+1}$ are all sol. to $P(-1)$: similar to $P(1)$-theorem]

- $P(-1)$: sufficient condition for solvability: $p=d=4k+1$ $\wedge$ d prime

[pr.: $\frac{x_1-1}{2}\frac{x_1+1}{2} = \left(\frac{y_1}{2}\right)^2$, $x_1+y_1\sqrt{p}$ f.s. to $P_p(1)$; $\frac{x_1\pm1}{2} = pv^2$; $\frac{x_1\mp1}{2} = v^2$, $\frac{y_1}{2} = uv$;
$v^2-pu^2 = \mp 1$; $+1$ ist ξ to $x_1+y_1\sqrt{p}$ f.s. of $P_p(1)$]

- $P(-1)$: necessary condition on d for solvability: $\nexists p = 4k+3$ prime: $p \mid d$

[pr.: $x^2-dy^2=-1 \Rightarrow \left(\frac{-1}{d}\right) \overset{!}{=} 1$ ξ]

- $P(4)$: form of solution: (x_1,y_1) f.s. $\Rightarrow \left(\frac{x_1+y_1\sqrt{d}}{2}\right)^n$ $n \in \mathbb{N}$ are all sol.

[pr. analogously to $P(1)$ case]

- connection f.s. of $P(4)$ and $P(1)$: (x_1,y_1) f.s. of $P(4) \Rightarrow$
$\begin{cases} \frac{x_1}{2}+\frac{y_1}{2}\sqrt{d} \text{ f.s. } P(1) & | x_1 \equiv_2 y_1 \equiv_2 0 \\ \frac{x_1}{2}+y_1\sqrt{d} \text{ f.s. } P_d(1) & | x_1 \equiv_2 0,\ y_1 \equiv_2 1 \\ *) & \left| \begin{array}{l} 4 \mid d = 4d' \\ \to \text{of } x^2-d'y^2=1 \end{array} \right. \end{cases}$

*) $x^2-dy^2=4$ has odd sol., (x_1,y_1) is f.s. $\wedge$ $d \equiv_8 5$ $\Rightarrow$

$\Rightarrow \left(\frac{x_1+y_1\sqrt{d}}{2}\right)^3 = \frac{1}{8}(x_1^3+3dx_1y_1^2) + \frac{1}{8}(3x_1^2y_1+dy_1^3)\sqrt{d}$ is f.s. to $P_d(1)$

[pr.: create ξ to $x_1+y_1\sqrt{d}$ f.s. to $P_d(4)$]

- $P(-4)$: form of solutions and connection to $P(4)$-sol.: (x_1,y_1) f.s. of $P_d(-4) \Rightarrow$

$\left(\frac{x_1+y_1\sqrt{d}}{2}\right)^n$ are $\begin{cases} \text{all sol. to } P_d(-4) & | \ n \in \mathbb{N}_u \\ \text{all sol. to } P_d(4) & | \ n \in \mathbb{N}_g \end{cases}$ in particular: $\left(\frac{x_1+y_1\sqrt{d}}{2}\right)^2$ is f.s. of $P_d(4)$

[pr.: analogously to $P(-1)$ and connection to $P(1)$]

- Finding the fundamental sol.: Let $\left(\frac{p_n}{q_n}\right)$ be the continued frac. expansion of $\sqrt{d}$

a) $p_n^2-dq_n^2 = (-1)^{n+1}t_{n+1}$ [as in chap. 8; pr.: $\sqrt{d} = \frac{\alpha_{n+1}p_n+p_{n-1}}{\alpha_{n+1}q_n+q_{n-1}} = \frac{(s_{n+1}+\sqrt{d})p_n+t_{n+1}p_{n-1}}{(s_{n+1}-\sqrt{d})q_n+t_{n+1}q_{n-1}}$

$\Rightarrow p_n^2-dq_n^2 = (p_nq_{n-1}-p_{n-1}q_n)t_{n+1} = (-1)^{n-1}t_{n+1}$

b) ℓ = length of period in cont. frac. exp. of $\sqrt{d}$:
i) $\ell \in \mathbb{N}_g$: no sol. to $P_d(-1)$; f.s. of $P_d(1)$ is $(p_{\ell-1}, q_{\ell-1})$
ii) $\ell \in \mathbb{N}_u$: f.s. to $P(-1)$: $(p_{\ell-1}, q_{\ell-1})$

Pellian equations:

a) facts: i) has either non or ∞ sol. [pr.: multiply with corresponding Pell eq. $P(1)$]

ii) $(x,y) \underset{\text{associated}}{\sim} (x',y') \Leftrightarrow xx' \equiv dyy' \pmod{N}$

b) Nagell's bound for $P_d(N)$ by $P_d(1)$: (u,v) f.s. to $P(1) \Rightarrow \forall (x^*,y^*)$ f.s. to $P_d(N)$:

i) $0 \le y^* \le \frac{v}{\sqrt{2(u+\varepsilon)}} \sqrt{|N|}$ ii) $|x^*| < \sqrt{\frac{1}{2}(u+\varepsilon)|N|}$ for $\varepsilon = \begin{cases} 1 & |N>0 \\ -1 & |N<0 \end{cases}$

[pr.: def. $x'+y'\sqrt{d} := (x^*+y^*\sqrt{d})(u-\delta v\sqrt{d})$, $\delta = \begin{cases} 1 & | x^*>0 \\ -1 & | x^*<0 \end{cases}$; use $y^* \in y'$]

XI, Polynomials

- division with rest [proof idea (pr.): induction $\deg(f)$ for $f = fg + r$; uniqueness: $(q_1 - q_2)g = r_2 - r_1$ $\Rightarrow$ ($\deg$ 0) $= r_2 - r_1$ ($\deg$ 0)]
- possible form of gcd in $K[X]$: $g = \gcd(f_1, f_2) = \rho_1 f_1 + \rho_2 f_2$ [$g := \rho_1 f_1 + \rho_2 f_2$ with min deg.; $\Rightarrow \deg(g) < \deg(1 f_1 + 0 f_2) = \deg(f_1) \Rightarrow f_1 = fg + r$ ($r = f_1 - fg = (1 - g\rho_1) f_1 + (-g\rho_2) f_2$) $\to r = 0 \Rightarrow g \mid f_1$]
- Gauss' lemma for polynomials: $\mathrm{cont}(fg) \sim \mathrm{cont}(f)\,\mathrm{cont}(g)$ [$f = c f_1$, $g = d g_1$, proof: $g_1 f_1$ primitive]
- primes = irreducible in UFD polynomial ring [$p \mid fg$; assume $p \nmid f$, consider $h \in \{bg + cf\}$, show $h = 0$ ($\deg(h) < \deg(g)$ minimality) $\Rightarrow hg = bgg + cfg = (bg + cf)g \Rightarrow p \mid hg \overset{\mathrm{cont}(p)=1}{\Rightarrow} p \mid f$]
- A UFD $\Rightarrow$ A[X] UFD:
[ex. of fact. per induction over $\deg(f)$; uniqueness of factorisation per induction over # irred. factors]
- lemma: The characteristic of an integral domain (ID) is 0 or a prime
[Assume $\mathrm{cha}(A) = n = n_1 n_2$, then $n \cdot 1 = (n_1 \cdot 1)(n_2 \cdot 1) = 0 \overset{A \text{ ID}}{\Rightarrow} n_1 = 0 \vee n_2 = 0 \Rightarrow \lightning$ minimality of $\mathrm{char}(A)$]
- theorem: exactly one zero of a polynomials root vanishes when taking the derivative for $\mathrm{cha}(A) = 0$:
[for $f(x) = (x-\alpha)^k g(x)$, $g(\alpha) \neq 0$: $f'(x) = (x-\alpha)^{k-1}((x-\alpha)g'(x) + k g(x))$]
- $\mathrm{Res}(f,g) = \det\begin{pmatrix} a_0 & 0 & b_0 & 0 \\ a_1 & a_0 & b_1 & b_0 \\ a_n & & & b_m \\ 0 & a_n & 0 & b_m \end{pmatrix} = a_0^m b_0^n \prod_{i,j}(\alpha_i - \beta_j) = a_0^m \prod_i g(\alpha_i) = b_0^n (-1)^{mn} \prod_j f(\beta_j)$
and $\mathrm{Res}(f = fg + r, g) = b_0^{\deg f - \deg r}\,\mathrm{Res}(r, g)$ [resultant]
- discriminant of a polynomial: $\mathrm{Disc}(f) = a_0^{2k-2} \prod_{i<j}(\alpha_i - \alpha_j)^2$; $a_0\,\mathrm{Disc}(f) = (-1)^{\frac{n(n-1)}{2}}\,\mathrm{Res}(f, f')$
- p polynomial irr. over $\mathbb{Q}[x] \Leftrightarrow p$ irr. over $\mathbb{Z}[x]$ [irr. $\mathbb{Q} \Rightarrow$ irr. $\mathbb{Z}$ obv.; $\mathbb{Z} \Rightarrow \mathbb{Q}$: Finde r, s: $\mathrm{cont}(rg) = \mathrm{cont}(sh) = 1$, $f = gh = $ bew. $\mathbb{Q}$, $rg, sh \in \mathbb{Z}[x]$ $\Rightarrow f = (rg)(sh)$ over $\mathbb{Z}$]
- correlation: rational root & coefficients of polynomial
[$\alpha = \frac{r}{s} \in \mathbb{Q}$ root of $f \Rightarrow r \mid a_n$; $s \mid a_0$]
- Schönemann criterion for irreducibility of polynomials: $f = g^n + ph \in \mathbb{Z}[x]$ with $g, h \in \mathbb{Z}[x]$, p prime, $n \in \mathbb{Z}$; f monic:
$\bar{g}$ irr. in $\mathbb{F}_p[x] \wedge \bar{g} \nmid \bar{h} \Rightarrow f$ irr. in $\mathbb{Z}$
[contraposition: $f = f_1 f_2 \overset{\text{in } \mathbb{F}_p[x]}{\Rightarrow} \bar{f} = \bar{f}_1 \bar{f}_2 = (\bar{g}^u + p h_1)(\bar{g}^v + p h_2) \overset{u \le v}{=} \bar{g}^n + \bar{g}^v h_3 + p h_1 h_2 \overset{\text{in } \mathbb{F}_p[x]}{=} \bar{g}^v h_3 + \bar{g}^n$
$\Rightarrow h = \bar{g}^v h_3 \Rightarrow \bar{g} \mid h$ $\lightning$]
- Eisenstein criterion: f monic $\in \mathbb{Z}[x]$, $p \mid a_{i \in 0..n-1}$, $p^2 \nmid a_0 \Rightarrow f$ irr. in $\mathbb{Z}[x]$
- Ritt's second theorem: all solutions to $a \circ b = c \circ d$ are i) $x^n \circ x^m \rho(x^n) = x^m \rho(x^n) \circ x^n$
ii) $D_n(x, a^m) \circ D_m(x, a) = D_{nm}(x, a) = D_m(x, a^n) \circ D_n(x, a)$ up to equivalence
where $D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}$ $\vee$ $D_n\left(z + \frac{a}{z}, a\right) = z^n + \left(\frac{a}{z}\right)^n$ is the Dickson polynomial

- Bilu & Tichy: classification of polynomial-pairs with ∞-many integer sols to $f(x)=g(y)$:

  $f(x)=g(y)$ has ∞-many rational sols with bounded denominator $\Leftrightarrow$ $f(x)=\varphi(f_1(\lambda(x)))$, $g(x)=\varphi(g_1(\mu(x)))$ with $f_1, g_1, \lambda, \varphi \in \mathbb{Q}[x]$, λ, μ linear, $\deg \varphi = 1$, (f_1, g_1) is a standard pair over $\mathbb{Q}$. Types of st. pairs:

  (1) $(x^n, ax^r p(x)^m)$ or switched : $0 \le r < m$, $\gcd(r,m)=1$, $r+\deg(p)>0$

  (2) $(x^2, (ax^2+b)p(x)^2)$

  (3) $(D_m(x, a^n), D_n(x, a^m))$. $\gcd(m,n)=1$

  (4) $(a^{-\frac{n}{2}} D_n(x,a), -b^{-\frac{n}{2}} D_n(x,b))$, $\gcd(m,n)=2$

  (5) $((ax^2-1)^3, 3x^4-4x^3)$

- f indecomposable over $\mathbb{Q} \Leftrightarrow$ f indec. over $\mathbb{C}$ [pr.: $f = h \circ g$ over $\mathbb{C}$; transform $f = h_1 \circ g_1$, g_1 monic; compare coeff. of f & $h_1 \circ g_1$ $\Rightarrow$ find $h_1 \in \mathbb{Q}[x]$]