Formulary

(Number Theory)

Introduction

This is the pdf-version of the Number Theory Formulary on MathLinks/ArtOfProblemSolving (http://www.mathlinks.ro/Forum/viewtopic.php?t=76610).
All contributors are welcome to post new theorems at http://www.mathlinks.ro/Forum/viewtopic.php?t=76609.
Contributers till now: $\{x\}$, Myth, pbornzstein, Schoppenhauer, mathmanman, Xixas, campos, t0rajir0u, bodan, dule_00.

Daniel (ZetaX), June 10, 2006

Contents

1 Symbols and conventions

1.1 Sets of numbers

$\mathbb{Z}$: the integers (a unique factorisation domain).
$\mathbb{N}$: the positive integers, meaning those > 0.
$\mathbb{P}$: the positive primes.
$\mathbb{Q}$: the rationals (a field).
$\mathbb{R}$: the reals (a field).
$\mathbb{C}$: the complex numbers (a algebraically closed and complete field).
$\mathbb{Q}_p$: the p-adic numbers (a complete field); also $\mathbb{Q}_0 := \mathbb{Q}$ and $\mathbb{Q}_\infty := \mathbb{R}$ is used sometimes.
$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$: the residues $\mod n$ (a ring; a field for n prime).

When M is one of the sets from above, then M^+ denotes the numbers > 0 (when defined), analogous for M^-.
The meaning of M^* will depend on M: for most cases it denotes the invertible elements, but for $\mathbb{Z}$ it means the nonzero integers (note that this definitions coincide in most cases).
A zero in the index, like in M_0^+, tells us that 0 is also included.

1.2 Definitions

1.2.1 General stuff

For a set M, $|M| = \#M$ denotes the number of elements of M.

a divides b (both integers) is written as $a|b$ or sometimes as $b \vdots a$.
Then for $m, n \in \mathbb{Z}$, $\gcd(m, n)$ or (m, n) is their **greatest common divisor**, the greatest $d \in \mathbb{Z}$ with $d|m$ and $d|n$ ($\gcd(0, 0)$ is defined as 0) and $\operatorname{lcm}(m, n)$ or $[m, n]$ denotes their **least common multiple**, the smallest non-negative integer d such that $m|d$ and $n|d$.
When $\gcd(m, n) = 1$, one often says that m, n are called "coprime".

For $n \in \mathbb{Z}^*$ to be "**squarefree**" means that there is no integer $k > 1$ with $k^2|n$. Equivalently, this means that no prime factor occurs more than once in the decomposition.

Factorial of n: $n! := n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 3 \cdot 2 \cdot 1$.
Binomial coefficients: $\binom{n}{k} = \frac{n!}{k!(n-k)!} = C_n^k$.

For two functions $f, g : \mathbb{N} \to \mathbb{C}$ the **Dirichlet convolution** $f * g$ is defined as $f * g(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$.
A (weak) **multiplicative function** $f : \mathbb{N} \to \mathbb{C}$ is one such that $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in \mathbb{N}$ with $\gcd(a, b) = 1$.
Some special types of such functions:
Euler's totient function: $\varphi(n) = \phi(n) := |\{k \in \mathbb{N} \;:\; k \leq n, \gcd(k, n)\}| = |\mathbb{Z}_n^*|$.
Moebius' function:
$$\mu(n) := \begin{cases} 0 \text{ iff } n \text{ is not squarefree} \\ (-1)^s \text{ where } s \text{ is the number of prime factors of } n \text{ otherwise} \end{cases}.$$
Sum of powers of divisors: $\sigma_k(n) := \sum_{d|n} d^k$; often τ is used for σ_0, the number of divisors, and simply σ for σ_1.

For any $k, n \in \mathbb{N}$ it denotes $r_k(n) := \left|\{(a_1, a_2, ..., a_k) \in \mathbb{Z}^k | \sum a_i^2 = n\}\right|$ the **number of representations of n as sum of k squares**.

Let a, n be coprime integers. Then $ord_n(a)$, the "**order of** $a \mod n$" is the smallest $k \in \mathbb{N}$ with $a^k \equiv 1 \mod n$.

For $n \in \mathbb{Z}^*$ and $p \in \mathbb{P}$, the **p-adic valuation** $v_p(n)$ can be defined as the multiplicity of p in the factorisation of n, and can be extended for $\frac{m}{n} \in \mathbb{Q}^*,\ m, n \in \mathbb{Z}^*$ by $v_p\left(\frac{m}{n}\right) = v_p(m) - v_p(n)$.
Additionally often $v_p(0) = \infty$ is used.

For any function f we define $\Delta(f)(x) := f(x+1) - f(x)$ as the (upper) finite difference of f. Then we set $\Delta^0(f)(x) := f(x)$ and then iteratively $\Delta^n(f)(x) := \Delta(\Delta^{n-1}(f))(x)$ for all integers $n \geq 1$.

1.2.2 Symbols

Legendre symbol: for $a \in \mathbb{Z}$ and odd $p \in \mathbb{P}$ we define
$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{when } x^2 \equiv a \mod p \text{ has a solution } x \in \mathbb{Z}_p^* \\ 0 & \text{iff } p|a \\ -1 & \text{when } x^2 \equiv a \mod p \text{ has no solution } x \in \mathbb{Z}_p \end{cases}$$
Then the **Jacobi symbol** for $a \in \mathbb{Z}$ and odd $n = \prod p_i^{v_i}$ (prime factorisation of n) is defined as: $\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right)^{v_i}$.

Hilbert symbol: let $v \in \mathbb{P} \cup \{0, \infty\}$ and $a, b \in \mathbb{Q}_v^*$. Then

$$(a,b)_v := \begin{cases} 1 & \text{iff } x^2 = ay^2 + bz^2 \text{ has a nontrivial solution } (x,y,z) \in \mathbb{Q}_v^3 \\ -1 & \text{otherwise} \end{cases}$$

is the "Hilbert symbol of a, b in respect to v" (nontrivial means here that not all numbers are 0).

1.2.3 Counting function and densities

When $A \subset \mathbb{N}$, then we can define a **counting function** $a(n) := |\{a \in A | a \leq n\}$.
One special case of a counting function is the one that belongs to the primes $\mathbb{P}$, which is often called π.
With counting functions, some types of densities can be defined:

Lower asymptotic density: ${}_L d(A) := \liminf_{n\to\infty} \frac{a(n)}{n}$
Upper asymptotic density: ${}_U d(A) := \limsup_{n\to\infty} \frac{a(n)}{n}$
Asymptotic density (does not always exist): $d(A) := \lim_{n\to\infty} \frac{a(n)}{n}$
Shnirelman's density: $\sigma(A) := \inf_{n\to\infty} \frac{a(n)}{n}$
Dirichlet's density(does not always exist): $\delta(A) := \lim_{s\to 1+0} \frac{\sum_{a\in A} a^{-s}}{\sum_{a\in\mathbb{N}} a^{-s}}$
${}_L d(A)$ and ${}_U d(A)$ are equal iff the asymptotic density $d(A)$ exists and all three are equal then and equal to Dirichlet's density.

Often, **density** is meant **in relation to some other set** B (often the primes). Then we need $A \subset B \subset \mathbb{N}$ with counting functions a, b and simply change n into $b(n)$ and $\mathbb{N}$ into B:

Lower asymptotic density: ${}_L d_B(A) := \liminf_{n\to\infty} \frac{a(n)}{b(n)}$
Upper asymptotic density: ${}_U d_B(A) := \limsup_{n\to\infty} \frac{a(n)}{b(n)}$
Asymptotic density (does not always exist): $d_B(A) := \lim_{n\to\infty} \frac{a(n)}{b(n)}$
Shnirelman's density: $\sigma_B(A) := \inf_{n\to\infty} \frac{a(n)}{b(n)}$
Dirichlet's density(does not always exist): $\delta_B(A) := \lim_{s\to 1+0} \frac{\sum_{a\in A} a^{-s}}{\sum_{a\in B} a^{-s}}$
Again the same relations as above hold.

2 Elementary congruences and divisors

Gauss' theorem :
If $a|bc$ and $\gcd(a,b)=1$, then $a|c$.

The Gauss' theorem comes from :
Bezout's identity :
The set $\{ax+by|x,y\in\mathbb{Z}\}$ is the set of all the multiples of $\gcd(a,b)$, that is to say :

$$a\mathbb{Z}+b\mathbb{Z}=\gcd(a,b)\mathbb{Z}$$

Fermat's little theorem:
For any positive integer a and every prime p it is $a^p \equiv a \mod p$.

Generalization:
Theorem of Euler-Fermat:
If $gcd(a,m)=1$ then $a^{\phi(m)} \equiv 1 \mod m$.

Wilson's theorem:
For prime p it is $(p-1)! \equiv -1 \mod p$.

Polynomial congruences:
For any polynom f with integral coefficients and any integers a,b with $a\equiv b \mod m$ for some integer m it is $f(a)\equiv f(b) \mod m$.

Lucas' theorem:
$\binom{a}{b} \equiv \prod_{i=0}^{k} \binom{a_i}{b_i} \mod p$ where a_i's and b_i's are the digits of a and b expressed in base p (p is a prime) with leading zeros allowed.

Wolstenholme's Theorem (number 1):
$\binom{2p}{p} \equiv 2 \mod p^3$ for $p\in\mathbb{P}\geq 5$

Wolstenholme's Theorem (number 2):
Let $\frac{m}{n}=1+\frac{1}{2}+\frac{1}{3}+...+\frac{1}{p-1}$ with $(m,n)=1$ and p is a prime greater than or equal to 5. Then p^2 divides m.

3 Identities

Identity of Sophie Germain:
For all integers a, b it is $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.

Sum-of-n-squares-identities:
- Two squares: $(a^2 + b^2)(c^2 + b^2) = (ac - bd)^2 + (ad + bc)^2$
- Four squares: $(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) =$
$(ae - bf - cg - dh)^2 + (af + be + ch - dg)^2 + (ag + ce + df - bh)^2 + (ah + de + bg - cf)^2$
- Eight squares:
$(a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2)(m^2 + n^2 + o^2 + p^2 + q^2 + r^2 + s^2 + t^2) =$
$u_1^2 + u_2^2 + u_3^2 + u_4^2 + u_5^2 + u_6^2 + u_7^2 + u_8^2$
where
$u_1 = am - bn - co - dp - eq - fr - gs - ht$
$u_2 = bm + an + do - cp + fq - er - hs + gt$
$u_3 = cm - dn + ao + bp + gq + hr - es - ft$
$u_4 = dm + cn - bo + ap + hq - gr + fs - et$
$u_5 = em - fn - go - hp + aq + br + cs + dt$
$u_6 = fm + en - ho + gp - bq + ar - ds + ct$
$u_7 = gm + hn + eo - fp - cq + dr + as - bt$
$u_8 = hm - gn + fo + ep - dq - cr + bs + at$
(see also http://www.geocities.com/titus_piezas/DegenGraves1.htm)

Similar to the previous ones:
$(a^2 + nb^2)(c^2 + nd^2) = (ac - nbd)^2 + n(ad + bc)^2$

Theorem: (Leibnitz):

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{\substack{k_1,\ldots,k_m > 0 \\ k_1+\cdots+k_m=n}} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}.$$

The Binet–Caushy identity:
For reals a_k, b_k, c_k, d_k we have

$$\left(\sum_{k=1}^{n} a_k c_k\right)\left(\sum_{k=1}^{n} b_k d_k\right) - \left(\sum_{k=1}^{n} a_k d_k\right)\left(\sum_{k=1}^{n} b_k c_k\right) = \sum_{1\le i<j\le n} (a_i b_j - a_j b_i)(c_i d_j - c_j d_i).$$

Vandermonde's identity:

$$\binom{m+n}{k} = \sum_{l=0}^{\max\{k,n\}} \binom{m}{k-l}\binom{n}{l}$$

Theorem (Vandermonde):
For the determinant

$$V_n(a_1, a_2, \ldots, a_n) = \begin{vmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ 1 & a_2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{vmatrix}$$

we have

$$V_n(a_1, a_2, \ldots, a_n) = \prod_{1 \le i \le j \le n} (a_j - a_i).$$

4 Floor function

On dealing with the floor function:
1. Let $n, m \in \mathbb{N}$, then

$$m \bmod n = m - n \cdot \left\lfloor \frac{m}{n} \right\rfloor$$

Remark: Perhaps this could work with $n, m \in \mathbb{R}$ but who would use it ?

2. Let $m \in \mathbb{N}, n \in \mathbb{Z}, x \in \mathbb{R}$, then

$$\sum_{k=0}^{m-1} \left\lfloor \frac{nk+x}{m} \right\rfloor = (m,n) \cdot \left\lfloor \frac{x}{d} \right\rfloor + \frac{m-1}{2} \cdot n + \frac{(m,n)-m}{2}$$

3. Let $m \in \mathbb{N}, x \in \mathbb{R}$, then

$$\lfloor m \cdot x \rfloor = \sum_{k=0}^{m-1} \left\lfloor x + \frac{k}{m} \right\rfloor$$

5 Number theoretic sums

Some number theorethic sum:

1. Let $n \in \mathbb{N}$
$$\sum_{j=1}^{n} \varphi(j) = \frac{3}{\pi^2} n^2 + O\left(n \log n\right)$$
$$\sum_{j=1}^{n} \varphi(j) = \frac{3}{\pi^2} n^2 + O\left(n \left(\log n\right)^{2/3} \left(\log \log n\right)^{4/3}\right)$$

2. Let $n \in \mathbb{N}$
$$\sum_{j=1}^{n} d\left(j\right) = n \log n + (2\gamma - 1)n + O\left(\sqrt{n}\right)$$

3. Let $n, k \in \mathbb{N}$
$$\sum_{j=1}^{n} \sigma_k(j) = \left(\frac{1}{k+1} \sum_{j=1}^{\infty} \frac{1}{j^{1+k}}\right) n^{1+k} + R_k(n)$$
where
$$R_k(n) = \begin{cases} O(n), \text{ when } 0 < k < 1 \\ O(n \log n), \text{ when } k = 1 \\ O(n^k), \text{ when } k > 1 \end{cases}$$

4. Let $n \geqslant 2$. Let $Q(n)$ denote the number of squarefree integers less than n. Then
$$Q(n) = \sum_{j=1}^{n} \mu^2(j) = \frac{6}{\pi^2} n^2 + O\left(\sqrt{n}\right)$$

5. Let f be a multiplicative function, if
$$S = \sum_{n=1}^{\infty} f(n)$$
converges absolutely, then
$$\prod_{p} \left(\sum_{k=0}^{\infty} f\left(p^k\right)\right) = \sum_{n=1}^{\infty} f(n)$$
where p runs through primes.

6. If f is completely multiplicative then
$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \frac{1}{1 - f(p)}$$
where p runs through primes.

7. Let f be a multiplicative function, then

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p))$$

$$\sum_{d|n} \mu^2(d) f(d) = \prod_{p|n} (1 + f(p))$$

where p is prime.

8. Let $n \in \mathbb{N}$, then

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1 \\ 0, & \text{if } n > 1 \end{cases}$$

9. Let $n \in \mathbb{N}$, then

$$\sum_{j=1}^{n} \frac{1}{\varphi(j)} = C_1 \log n + C_2 + O\left(\frac{\log n}{n}\right)$$

where $C_1 > 0$ and C_2 are real constants.

10. Let $n \in \mathbb{N}$, then

$$\sum_{j=1}^{n} \omega(j) = n \log\log n + Bn + O\left(\frac{n}{\log n}\right)$$

$$\sum_{j=1}^{n} \Omega(j) = n \log\log n + (B + C)n + O\left(\frac{n}{\log n}\right)$$

$$\sum_{j=1}^{n} \omega^2(j) = n \left(\log\log n\right)^2 + O\left(n \log\log n\right)$$

where B, C are constants.

11. Let $n \in \mathbb{N}$, then

$$(\log\log x) - 1 \leqslant \sum_{p \leq x} \frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right)$$

where p runs through primes and B is a constant.

$$\sum_{k \geq 2, p^k \leq x} \frac{1}{p^k} = C + O\left(\frac{1}{\log x}\right)$$

where p runs through primes and C is a constant.

12. Let $n \in \mathbb{N}$, then

$$\sum_{n \leq x} r_2(n) = \pi x + O\left(x^{1/3} \log x\right)$$

Let $n \geqslant 2$ be a positive integer, then

$$\sum_{p \leq n} \frac{\log p}{p} = \log n + O(1)$$

where p runs through primes.

13. Let $z \in \mathbb{C}$, and $n \in \mathbb{N}$, then

$$\prod_{p \leq n} \left(1 + \frac{z}{p}\right) = A(z) \left(\log n\right)^z \cdot \left(1 + O\left(\frac{1}{\log n}\right)\right)$$

for $A(z)$ a constant depending on z.

14. Let $n \in \mathbb{N}$, then

$$\sum_{d|n} \frac{1}{d} \geqslant \frac{n}{2\varphi(n)}$$

15. Let k, l be two positive integers with $(k, l) = 1$, then

$$\sum_{\substack{p \leq x \\ p \equiv l (\mod k)}} \frac{1}{p} = \frac{1}{\varphi(k)} \log \log x + O(1)$$

where p runs through primes.

16. Let f be an additive function and n a positive integer, then

$$\sum_{m \leq n} \left(|f(m) - \sum_{p \leq n} \frac{f(p)}{p}| \right)^2 \leqslant Cn \sum_{p^k \leq n} \frac{|f\left(p^k\right)|^2}{p^k}$$

where p runs through primes, and C is a constant ($C \leqslant 32$).

17. Let f be a strongly additive function, and n a positive integer. Then

$$\sum_{m \leq n} \left(|f(m) - \sum_{p \leq n} \frac{f(p)}{p}| \right)^2 \leqslant 2Cn \sum_{p \leq n} \frac{|f(p)|^2}{p}$$

where p runs through primes and C is a constant ($C \leqslant 32$).

Some other sums 1. **Abelian summation**

Let $(a_j)_{j=1}^{n}, (b_j)_{j=1}^{n}$ be a finite sequence of complex numbers. Then

$$\sum_{i=1}^{n} a_i b_i = \left(\sum_{i=1}^{n} a_i\right) b_n - \sum_{m=1}^{n-1}\left(\left(\sum_{i=1}^{m} a_i\right)(b_{m+1} - b_m)\right)$$

2. Let $(a_m)_{m=1}^{n}, (b_m)_{m=1}^{n}$ be two finite sequence of real numbers. Then

$$\left(\sum_{k=1}^{n} a_k\right)\cdot\left(\sum_{k=1}^{n} b_k\right) = n\sum_{k=1}^{n} a_k b_k - \sum_{k=2}^{n}\sum_{j=1}^{k-1}(a_k - a_j)\cdot(b_k - b_j)$$

Or equivalently

$$\left(\sum_{k=1}^{n} a_k\right)\cdot\left(\sum_{k=1}^{n} b_k\right) = n\sum_{k=1}^{n} a_k b_k - \sum_{1\leq j<k\leq n}(a_k - a_j)\cdot(b_k - b_j)$$

3. Let $n \in \mathbb{N}$

$$\ln n + \gamma + \frac{1}{2n} \leqslant \sum_{j=1}^{n}\frac{1}{j} = \ln n + \gamma + \frac{1}{2n} + O\left(\frac{1}{n^2}\right)$$

Where $\gamma = \lim\limits_{n\to\infty}\left(\sum_{j=1}^{n}\frac{1}{j} - \ln n\right)$ is the gamma constant.

6 Arithmetic functions

1. Let $n \in \mathbb{N}$, then

$$\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) = \sum_{d|n}\mu(d)\frac{n}{d}$$

2. Let $n \in \mathbb{N}$, then

$$\frac{1}{\varphi(n)} = \frac{1}{n}\sum_{d|n}\frac{\mu^2(d)}{\varphi(d)}$$

3. Let $n \in \mathbb{N}$, then

$$0,92129\cdot\frac{n}{\log n} < \pi(n) < 1,1055\cdot\frac{n}{\log n}$$

4. Let $n \in \mathbb{N}$, then
$$\frac{6}{\pi^2}n^2 \leq \sigma(n)\varphi(n) \leq n^2$$

5. Let $n \geqslant 2$ be a positive integer, then
$$\varphi(n) \geqslant \frac{cn}{\log\log n}$$
for some positive constant $c > 0$.

6. For all composite numbers n it holds
$$\varphi(n) \leq n - \sqrt{n}$$

7. Let p_n be the n-th prime number, then
$$an\log n \leqslant p_n \leqslant bn\log n$$
for two constants $0 < a < b$.

8. Let n be a positive integer, then
$$\omega(n) \leqslant \lg_2 n$$

9. Let n be a positive integer, then
$$d(n) \leqslant 2\sqrt{n}$$

7 Sums of squares

2) Sum of two squares:
A positive integer n can be represented as sum of two perfect squares iff all prime factors $p \equiv 3 \mod 4$ of n occur an even number of times in the factorisation of n. n can be written as sum of squares $\neq 0$ iff the previous condition holds and it has at least one prime factor $\equiv 1 \mod 4$ or $v_2(n)$ is odd.
There are exactly
$$\mathrm{r}_2(n) = 4 \cdot \sum_{\substack{d \in \mathbb{N} \\ d \mid n \\ d \equiv 1 \mod 2}} (-1)^{\frac{d-1}{2}} = 4 \cdot \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \mod 4}} (v_p(n) + 1)$$

different solutions $(a, b) \in \mathbb{Z}^2$ to $n = a^2 + b^2$.

3) Sum of three squares:
Write n as $n = 4^k u$, $k, u \in \mathbb{N}_0$ with $4 \nmid u$ (but u can be even). Then n can be written as sum of three squares iff $u \not\equiv 7 \mod 8$.

4) Sum of four squares:
Every positive interger can be written as sum of four squares, and there are

$$\mathrm{r}_4(n) = 8 \cdot \sum_{\substack{d \in \mathbb{N} \\ 4 \nmid d | n}} d = \begin{cases} 8\sigma(n) \text{ iff } n \text{ is odd} \\ 24\sigma(n) \text{ iff } n \text{ is even} \end{cases}$$

different solutions $(a, b, c, d) \in \mathbb{Z}^4$ to $n = a^2 + b^2 + c^2 + d^2$.

5) Sum of five squares:
As corollary to 4) every integer can be written as sum of five squares, but there is one more thing to say: except of some small numbers (all < 100), every positive integer can be written as sum of five nonzero perfect squares.

8) Sum of eight squares:
There are

$$\mathrm{r}_8(n) = 16 \cdot \sum_{\substack{d \in \mathbb{N} \\ d | n}} (-1)^{n-d} d^3$$

different solutions $(a, b, c, d, e, f, g, h) \in \mathbb{Z}^8$ to $n = a^2 + b^2 + c^2 + d^2 + e^2 + f^2 + g^2 + h^2$.

8 p-adic numbers, Hasse-Minkowski

p-adic numbers

The p-adic integers (for that and only that post written by $\mathbb{Z}_p$) are isomorphic (or by definition identical) to:
a) the (formal) series $\sum_{k=0}^{\infty} a_k p^k$ with $a_k \in \{0, 1, 2, ..., p-1\}$.
b) the cauchy-sequences $(b_k)_{k \in \mathbb{N}_0}$ of integers in respect to the p-adic valuation $|\cdot|_p = p^{-v_p(\cdot)}$.
c) the projective limit $\lim_{\leftarrow n} \mathbb{Z}/p^n\mathbb{Z}$.

The last one gives that a polynomial equation $p(x) = p(x_1, x_2, ..., x_n)$ has a solution in $\mathbb{Z}_p$ iff it has one $\mod$ any power of p.

The p-adic numbers $\mathbb{Q}_p$ are isomorphic (or by definition identical) to:
a) the (formal) series $\sum_{k=-s}^{\infty} a_k p^k$ with $a_k \in \{0, 1, 2, ..., p-1\}$.
b) the rational cauchy-sequences $(b_k)_{k\in\mathbb{N}_0}$ in respect to the p-adic valuation $|\cdot|_p = p^{-v_p(\cdot)}$.
c) the field of quotients of $\mathbb{Z}_p$.

Some properties of the Hilbert symbol (holding for any $v \in \mathbb{P} \cup \{0, \infty\}$ and $a, b, c \in \mathbb{Q}_v^*$):
- $(a, b)_v = (b, a)_v$
- $(a, 1)_v = 1 = (1, b)_v$
- $(a, bc^2)_v = (a, b)_v = (ac^2, b)_v$
- $(a, bc)_v = (a, b)_v \cdot (a, c)_v$

Product formula for the Hilbert symbols:
Let a, b be rational. Then $(a, b)_v = 1$ for all but finetely many $v \in \mathbb{P} \cup \{\infty\}$ and:

$$\prod_{v\in\mathbb{P}\cup\{\infty\}} (a, b)_v = 1$$

Approximation of the Hilbert Symbols: Let a finite set $\{a_1, a_2, ..., a_k\}$ of rational numbers and then for all $j \in K := \{1, 2, ..., k\}$ and $v \in \mathbb{P} \cup \{\infty\}$ an $e_{j,v} \in \{\pm 1\}$ be given such that:
- all but finetely many $e_{j,v}$ are equal to 1
- for any $j \in K$ it holds $\prod_{v\in\mathbb{P}\cup\{\infty\}} e_{j,v} = 1$
- there is an $x_v \in \mathbb{Q}_v^*$ such that $(a_{j,v}, x_v)_v$ for all $j \in K$

Then there exists a rational number x with $(a_{j,v}, x)_v = e_{j,v}$ for all (j, v).

The theorem of Hasse-Minkowski:
Let $f(x) = f(x_1, x_2, ..., x_n) = 0$ be any homogenous polynomial equation of degree 2 (so f is a polynomial where every single monomial has degree 2).
Then there exists a nontrivial (not all numbers = 0) rational solution $x \in \mathbb{Q}^n$ to $f(x) = 0$ iff this equation has a nontrivial solution $x \in \mathbb{Q}_v^n$ for all $v \in \mathbb{P} \cup \{\infty\}$.

Corollary: when f has also integer coefficients, the equation $f(x) =$ has a nontrivial integral solution iff it has a solution $\mod$ any integer (where by the Chinese Remainder Theorem we can restrict to perfect powers of primes).

9 Legendre's and Jacobi's symbols, quadratic reciprocity law

Basic facts on the Legendre's and Jacobi's symbols. The quadratic reciprocity law.

Theorem 1.
If $a \equiv b \pmod p$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Theorem 2.
For all $a \not\equiv 0 \pmod p$ we have $\left(\frac{a^2}{p}\right) = +1$.

Theorem 3 (Euler's criteria).
$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

Theorem 4.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1, & p = 1 \pmod 4), \\ -1, & p = 3 \pmod 4). \end{cases}$$

Theorem 5.

$$\left(\frac{a_1 a_2 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right).$$

Theorem 6 (Gauss criteria).
For all $a \neq 0 \pmod p$, $p > 2$, the following equality holds

$$\left(\frac{a}{p}\right) = (-1)^l,$$

where $l = |\{ak \mid 1 \leq k \leq \frac{p-1}{2},\ ak \pmod p \geq \frac{p+1}{2}\}|$.

Theorem 7.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} +1, & p = 8k \pm 1, \\ -1, & p = 8k \pm 3. \end{cases}$$

Theorem 8 (The quadratic reciprocity law).
For all odd primes $p \neq q$ the following equality holds:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Definition.
Let odd $m = p_1 p_2 ... p_s$, where p_i are prime number, not necessary distinct, $(a, m) = 1$. Then Jacobi's symbols $\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) ... \left(\frac{a}{p_s}\right)$, where $\left(\frac{a}{p_i}\right)$ are Legendre's symbols.

Theorem 1'.
The same as Theorem 1 for Legendre's symbol.

Theorem 2'.
The same as Theorem 2 for Legendre's symbol.

Theorem 4'.

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} +1, \, m = 1 \pmod 4, \\ -1, \, m = 3 \pmod 4. \end{cases}$$

Theorem 5'.

$$\left(\frac{a_1 ... a_s}{m}\right) = \left(\frac{a_1}{m}\right) ... \left(\frac{a_s}{m}\right).$$

Theorem 7'.

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} +1, \, m = 8k \pm 1, \\ -1, \, m = 8k \pm 3. \end{cases}$$

Theorem 8' (The reciprocity law for Jacobi's symbols).
Let m, n be odd numbers, $m, n > 1$, then

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}.$$

10 Representations

In base b:
Every $n \in \mathbb{N}_0$ can be uniquely written in base b, meaning $n = \sum_{k=0}^{\infty} a_k b^k$ with all $a_k \in \{0, 1, 2, ..., b-1\}$ and all but finetely many $a_k = 0$.

Zeckendorf's (base Fibonacci) representation:
Every $n \in \mathbb{N}$ can be uniquely expressed as a sum of Fibonacci numbers no two of which are consecutive.

Waring's Theorem:

Let $f : \mathbb{N}_0 \to \mathbb{N}_0$ by a polynomial and let $d = \gcd(f(0), f(1), f(2), ...)$. Then every sufficient large multiple of d can be expressed as sum of a bounded number of values of f, or in other words: there is a k only depending on f such that for any $n > N$ (N some constant) there are $a_1, a_2, ..., a_k \in \mathbb{N}_0$ with $dn = f(a_1) + f(a_2) + ... + f(a_k)$. Especially when 0 and 1 are in the range of f, then every $n \in \mathbb{N}_0$ can be written as a bounded number of values of f. Addionally, for any m there is a k such that any $n \in \mathbb{N}_0$ is the sum of k non-negative m-th powers of integers.

Related to Waring's Theorem:
- every positive integer is the sum of 4 perfect squares (see also the Sum of Squares section).
- every positive integer is the sum of 3 triangular numbers (those of type $\frac{n(n+1)}{2}$).
- every integer is the sum of 9 non-negative perfect cubes.
- every integer is the sum of 5 perfect cubes (they are allowed to be negative). It's an openen problem if 4 cubes suffice.

11 p-adic valuations

Let p be any fixed prime for this section.

Properties of v_p:
For all rational a, b:
$v_p(ab) = v_p(a) + v_p(b)$
Non-archimead triangle inequality: $v_p(a + b) \geq min(v_p(a), v_p(b))$

Hensel's lemma:
$p^s||a - 1,\ p^k||b,\ s \geq 1 \ \Rightarrow\ p^{s+k}||a^b - 1$, or in other words $v_p(a^b - 1) = v_p(a - 1) + v_p(b)$ for $v_p(a - 1) \geq 1$, with exception of the case $p = 2,\ s = 1$.

Kummer's theorem:
If $p^s|\binom{n}{n-k}$ then s does not exceed the number of carries needed when the numbers $n - k$ and k are added when expressed in base p.

12 Primes

Bertrands postulate

There is always a prime between n and $2n$ ($n \in \mathbb{N}$).

Chebychevs Theorem:
There are constants a, b, $0 < a < b$ such that for all big n (e.g. $a = \log(2), b = \log(4)$ for $n \geq 2$) we have

$$a \cdot n \leq \pi(n) \cdot \log(n) \leq b \cdot n$$

Prime number theorem
There are asymptotically $\frac{x}{\log(x)}$ primes $\leq x$.

Dirichlet's theorem on primes in arithmetic progression:
In every arithmetic progression $an + b$ with $\gcd(a, b) = 1$ there are infinitely many primes. More exactly, the asymptotic and Dirichlet's densities of these primes in the set of all primes are $\frac{1}{\phi(n)}$.

Zsigmondy's Theorem:
Let $a > b \geq 1$ and be coprime integers. Then for any $n \in \mathbb{N}$ there is a prime p dividing $a^n - b^n$ but not dividing $a^k - b^k$ for all $k < n$ with two exceptions: a) $a = 2,\ b = 1,\ n = 6$ b) $a + b$ a power of 2 and $n = 2$

13 Additive properties

The Theorem of Chevalley-Warning:
Let be p prime and $f_1, f_2, ..., f_m$ be m polynomials with integer coefficients in the n variables $x = (x_1, x_2, ..., x_n)$. If $\sum_{i=1}^{m} \deg(f_i) < n$, then the number of solutions of

$$f_1(x) \equiv 0 \mod p$$

$$f_2(x) \equiv 0 \mod p$$

$$...$$

$$f_m(x) \equiv 0 \mod p$$

is divisible by p (this generalizes to any finite field).

The Cauchy-Davenport Theorem:
Let p be prime and $A, B \subset \mathbb{Z}/p\mathbb{Z}$. Then the following inequality holds for the sumset $A + B$:

$$|A + B| \geq \min(p, |A| + |B| - 1)$$

Vosper's Theorem (the case of equality in the Cauchy-Davenport Theorem):
With the conditions above and $A + B \neq \mathbb{Z}/p\mathbb{Z}$, we have $|A+B| = |A| + |B| - 1$ if and only if one of the following is true:
a) $|A| = 1$ or $|B| = 1$
b) $|A+B| = p-1$ and $B = (\mathbb{Z}/p\mathbb{Z})\backslash(c-A)$, where c is the only one residue class $\notin A+B$
c) A and B are (seen $\mod p$) arithmetic progressions with the same common difference

Some results that follow from the above:

The Erdös-Ginzburg-Ziv Theorem:
Let $n \in \mathbb{N}$ and $2n-1$ integers be given. Then we can choose exactly n of them such that their sum is divisible by n.

Sums of k-th powers $\mod p$:
Let p be prime and $k \in \mathbb{N}$. Then $\mod p$ any number is the sum of k k-th powers, or in other words: for any $n \in \mathbb{Z}$, there are integers $a_1, a_2, a_3, ..., a_k$ with $n \equiv a_1^k + a_2^k + a_3^k + ... + a_k^k \mod p$.

Sharper version of the previous one:
With the same conditions as before, extended by $p \geq 5$, $1 < k < \frac{p-1}{2}$ and $k|p-1$ (it's clear that the condition $k|p-1$ is no restriction), and any $n \in \mathbb{N}$ we have that there are at least $\min\big(p, (2n-1)\frac{p-1}{k} + 1\big)$ residues that are the sum of n k-th powers.

14 Multiplicative functions

Theorem(Ramanujan):
For $(m,n) \in \mathbb{N}^2$:

$$\sum_{d|gcd(m,n)} d\mu(\frac{n}{d}) = \frac{(\frac{n}{gcd(m,n)})\phi(n)}{\phi(\frac{n}{gcd(m,n)})}$$

15 Irreducibility of polynomials

Theorem (Eisenstein) Suppose we have the following polynomial with integer coefficients:

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

If there exists a prime p such that $p|a_j,\ j \in \{0, 1, 2, \ldots, n-1\},\ \ p \nmid a_n$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible.

16 Finite differences

Formula for $\Delta^n(f)$:

$$\Delta^n f(x) = \sum_{r=0}^{n} (-1)^{n-r} \binom{n}{r} f(x+r)$$

Effect on degrees of polynomials:
When P is a polynomial of degree n, then $\Delta^k(P)$ is a polynomial of degree $n-k$, where negative degrees mean the constant polynomial 0 everytime.