素数和合数

1. 任一数 $a>1$, $a\in N$, 则 $a>1$ 的最小因数为质数 p

2. a 为合数, $p\le\sqrt{a}$

   证明: 设 $a=pq$, $p\le q$ $\therefore a=pq\ge p^2$, $p\le\sqrt{a}$

3. 埃氏筛法:

   如找30以内素数, $5<\sqrt{30}<6$, 所以 $(2,3,5)$ 作为筛子

4. Th. (Euclid) 素数有无限多个。

   证明: 设最大为 p_k, 令 $N=p_1p_2\cdots p_k+1$, 易知 $p_1\sim p_k\nmid N$

5. 性质

   (1) $(p,a)=1$ 或 $p\mid a$

   (2) $p\mid ab \Rightarrow p\mid a$ 或 $p\mid b$

   证明: 若 $p\nmid a$, $p\nmid b$, 则 $(p,a)=1$, $(p,b)=1$

   $\therefore (p,ab)=1$, $\therefore p\nmid ab$, 矛盾

   证: 有两种情况

   ① $p\nmid a \Leftrightarrow (p,a)=1$, $\Rightarrow p\mid b$

   ② $p\mid a$

   $\therefore p\mid a$ 或 $p\mid b$

6. 算术基本定理: $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$

   若 $d\mid n$, $d=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$, 则 $0\le\beta_i\le\alpha_i$

   1° $\tau(n)=\prod_{i=1}^{k}(\alpha_i+1)$, $\tau(n)$ 表示 n 的正因子个数

   2° $\sigma(n)=(1+p_1+p_1^2+\cdots+p_1^{\alpha_1})(1+p_2+\cdots+p_2^{\alpha_2})\cdots(1+p_k+\cdots+p_k^{\alpha_k})$

   $=\prod_{i=1}^{k}(1+p_i+\cdots+p_i^{\alpha_i})$

   $=\prod_{i=1}^{k}\frac{1-p_i^{\alpha_i}}{1-p_i}$, $\sigma(n)$ 表示 n 的所有正因子之和

7. 若 $\sigma(n)=2n$, 称 n 为完美数 (perfect number), $(6, 28, 496, 8128\cdots)$

8. 设 p 在 $n!$ 标准分解中出现的次数为 α, 则有

   $$\alpha=\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$$

   $$\therefore n!=\prod_{p\le n}p^{\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]}$$

9. n 为平方数 $\Leftrightarrow \tau(n)$ 为奇数

   证明: $(\Rightarrow)$ 设 $n=m^2$, $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$

   $\therefore m^2=p_1^{2\alpha_1}p_2^{2\alpha_2}\cdots p_k^{2\alpha_k}$

   $\therefore \tau(n)=\prod_{i=1}^{k}(2\alpha_i+1)$, 为若干个奇数之积

   $\therefore \tau(n)$ 为奇

(二) 若将 n 写作 $p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，设其不是完全平方数

$\therefore$ $\alpha_1,\alpha_2,\cdots,\alpha_k$ 中不全为偶，否则令 $t=p_1^{\frac{\alpha_1}{2}}p_2^{\frac{\alpha_2}{2}}\cdots p_k^{\frac{\alpha_k}{2}}$，

则有 $n=t^2$，矛盾

$\therefore$ $\tau(n)=\prod_{i=1}^{k}(\alpha_i+1)$，为偶。

$\therefore$ n 不是完全平方数 $\Rightarrow$ $\tau(n)$ 为偶

$\therefore$ $\tau(n)$ 为奇 $\Rightarrow$ n 是完全平方数

同余

(6) $ac\equiv bc \pmod m$，记 $(c,m)=d$，$a\equiv b \pmod{\frac{m}{d}}$

(7) $a\equiv b \pmod m$，$a\equiv b \pmod n$，则 $a\equiv b \pmod{[m,n]}$

(8) $\left.\begin{array}{l} a\equiv b \pmod m,\ n\mid m \\ \hookrightarrow m\mid a-b \end{array}\right\} \longrightarrow n\mid a-b$

例：求 $(257^{33}+46)^{26} \bmod 50$

解：$(257^{33}+46)^{26} \equiv (7^{33}+46)^{26}$

$\equiv [(-1)^{16}\times 7-4]^{26}$

$\equiv 3^{26}$

$\equiv 3^{20}\times 3^{6}$

$\equiv 3^{6}$

$\equiv 29 \pmod{50}$

费马小定理：$p\mid n^p-n$，$n\in Z, p\in P$.

第二课时　素数与合数

一、知识梳理

1. 大于 1 的整数n至少有两个不同的正约数. 如果n只有两个不同的正因子, 那么称n为素数; 如果n不是素数, 那么称n为合数.

2. 任一数$a>1$, 且$a\in N$, 则a大于 1 的最小因数是质数p.

3. Euclid 定理 素数有无穷多个!

4. 素数的性质

(1) 设p为素数, $n\in Z$, 那么$p\mid n$或$(p,n)=1$.

(2) 设p为素数, 且$p\mid ab$, 那么$p\mid a$, 或$p\mid b$.

5. 算术基本定理 设$n\geq 2$, 那么n可以写成一些素数的积. 如果不考虑乘积的顺序, 这种表示法是唯一的, 即$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$, 其中$p_1,p_2,\cdots p_t$是互不相同的素数, $\alpha_1,\alpha_2,\cdots\alpha_t$是正整数.

二、经典例题

例 1 构造 30 以内的质数表.

$\cancel{1}$ 2 3 $\cancel{4}$ 5 $\cancel{6}$ 7 $\cancel{8}$ $\cancel{9}$ $\cancel{10}$

11 $\cancel{12}$ 13 $\cancel{14}$ $\cancel{15}$ $\cancel{16}$ 17 $\cancel{18}$ 19 $\cancel{20}$

$\cancel{21}$ $\cancel{22}$ 23 $\cancel{24}$ $\cancel{25}$ $\cancel{26}$ $\cancel{27}$ $\cancel{28}$ 29 $\cancel{30}$

例 2 设a,b为互素的整数, 则$(a^2+b^2,ab)=1$.

解: ~~设 $p\mid a^2+b^2$ 且 $p\mid ab$, $p\in P$~~

∴ ~~$p\mid a^2+b^2-2ab$~~

∴ ~~$p\mid(a+b)^2$~~

∴ ~~$p\mid a+b$ ∴ $p\mid a$ 且 $p\mid b$~~

~~又∵ $(a,b)=1$~~

∴ ~~矛盾 ∴ $(a^2+b^2,ab)=1$~~

∵ $(a,b)=1$

∴ $(a,b\times b)=(a,b^2)=(a,b)=1$

∴ $(a,a^2+b^2)=1$

同理 $(b,a^2+b^2)=1$

∴ $(a^2+b^2,ab)=1$

设 $p\mid a^2+b^2$ 且 $p\mid ab$, $p\in P$

∴ $p\mid a^2+b^2+2ab$

$p\mid(a+b)^2$

∴ $p\mid a+b$

∵ $p\mid ab$ ∴ $p\mid a$ 或 $p\mid b$

∵ $p\mid a+b$ ∴ $p\mid a, p\mid b$

又∵ $(a,b)=1$, $1\notin P$

∴ 矛盾 ∴ $(a^2+b^2,ab)=1$

例 3　求所有的素数 p，使得 $2p+1$ 和 $4p+1$ 都是素数.

解：$p=2$ 时，不成立

$p=3$ 时，$2p+1=7$，$4p+1=13$，成立

$p>3$ 时，~~设 $p=2k+1$~~

∴ ~~$2p+1=4k+3$ 若 $3\nmid 2p+1$~~，

则 $p=3k+1$ 或 $3k+2$，$k\in N^*$

若 $p=3k+1$，则 $3\mid 2p+1$

若 $p=3k+2$，则 $3\mid 4p+1$，

∴ 不存在 $p>3$ 满足条件　∴ 综上，$p=3$

例 4 求 20! 的标准素因数分解式.

解：小于20的素数：2, 3, 5, 7, 11, 13, 17, 19

在 1~20 中，有 $\frac{20}{2}=10$ 个为 2 的倍数，

这 10 个中，有 $\frac{10}{2}=5$ 个为 2^2 的倍数

这 5 个中，有 $[\frac{5}{2}]=2$ 个为 2^3 的倍数

……，有 $\frac{2}{2}=1$ 个为 2^4 的倍数

∴ 20! 的分解中有 $10+5+2+1=18$ 个

同理，有 8 个 3，4 个 5，2 个 7，其余皆为 1 个

∴ $20! = 2^{18}\times 3^8\times 5^4\times 7^2\times 11\times 13\times 17\times 19$

例 5. 求证：存在连续 100 个正整数，它们都是合数.

证明：任取连续 100 个自然数 $k_1, k_2, \cdots k_{100}$，$k_1\geq 2$

并记 $k_1k_2\cdots k_{100}=n$

易知 $n+k_1$，$n+k_2$，…，$n+k_{100}$ 为满足条件的 100 个整数

三、巩固练习

1. 构造 100 以内的质数表.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100					

2. 证明：有无穷多个 $4k-1$ 形式的素数.

证明：设只有有限多个，且为 $k_1, k_2, \cdots, k_n$

令 $N = 4(k_1k_2\cdots k_n)-1$

i N 为素数

又∵ $N > k_n$，矛盾

ii N 为合数，~~设p~~

若 $p>2$ 且 $p\in P$，则 $p=4k+1$ 或 $4k-1$

∵ ~~$(4k+1)(4k'+1)$~~，$k, k' \in N^*$

∴ N 不为若干个 $4k+1$ 之积

∴ $\exists\, p_0 = 4k_0-1$，$p_0 | N$

若 $p_0 \in P_{k_i}$，则 $p_0 | p_0-1$，显然矛

若 $p_0 \notin P_{k_i}$，则 $p_0 > k_n$

与假设矛盾

∴ 综上，有无穷多个

若所有 $p_i | N$ 都是 $4k+1$ 的形式，则 N 也是 $4k+1$ 的形式

3. 如果一个素数即可以表示成两个素数的和，又可以表示成两个素数的差，求所有这样的素数.

解：~~p=~~ ∵ p 可以表示成两素数之和

∴ $p>2$

∴ p 为奇数 ∴两数中必有一个2

$p=3$ 时，$3=2+1$，舍

$p=5$ 时，$5=2+3=7-2$，成立

下面证明 $p>5$ 时，不可能满足条件

若 $p=3k+1$，则 $3|(3k+1)+2$，舍

若 $p=3k+2$，则 $3|(3k+2)-2$，舍

综上，不可能　∴只有5

4. 证明：大于 11 的整数可以表示成两个合数的和.

证明：设其为 $n+11$ [illegible]

~~若n为奇，则 2|n+11~~

若 $n=3k+1$，则 $n+11=3k+12$，$3k$ 和 12 为合数

若 $n=3k$，则 $n+11=3(k+1)+8$，$3(k+1)$ 和 8 为合数

若 $n=3k+2$，则 $n+11=3(k+1)+10$，$3(k+1)$ 和 10 为合数

综上，命题得证

5. 50! 的十进制表示式中结尾有多少个零？

解：~~$\frac{50}{10}=5$，$\frac{5}{10}=0$，有10^5作为因子~~

$\left[\frac{50}{2}\right]+\left[\frac{50}{4}\right]+\left[\frac{50}{8}\right]+\left[\frac{50}{16}\right]+\left[\frac{50}{32}\right]=25+12+6+3+1=47$，有$2^{47}$作为因子

$\left[\frac{50}{5}\right]+\left[\frac{50}{25}\right]=12$，有$5^{12}$作为因子

∴ 有12个。

6. 证明：若正整数 m、n 满足 $(m,n)+[m,n]=m+n$，则 m 与 n 中的一个数是另一个数的倍数.

证明：不妨设 $m \le n$

∵ $\begin{cases}(m,n)[m,n]=mn \\ (m,n)+[m,n]=m+n\end{cases}$

∴ (m,n) 为和 $[m,n]$ 为方程 $x^2-(m+n)x+mn=0$ 的两根

∵ $(m,n) \le [m,n]$

∴ $(m,n)=m$，$[m,n]=n$

∴ n 是 m 的倍数

7. 设正整数 a、b、x、y 满足 $\left(a^2+b^2\right)\mid(ax+by)$. 证明：$x^2+y^2$ 与 a^2+b^2 不互素。

证明：~~∵ $(a^2+b^2)a \mid (ax+by)$~~

~~∴ 设 $a^2+b^2=k(ax+by)$~~

~~若 x^2+y^2 与 a^2+b^2 互素~~

~~则 $(a^2+b^2, x^2+y^2)=1$~~

∴ ~~$(a^2+b^2, x^2+y^2 \ldots) \ne 1$~~

∵ $(a^2+b^2)\mid(ax+by)$

∴ $(a^2+b^2)\mid(ax+by)(bx+ay)$

∴ $(a^2+b^2)\mid ab(x^2+y^2)+xy(a^2+b^2)$

∴ $a^2+b^2 \mid ab(x^2+y^2)$

∵ $a^2+b^2>ab>0$

∴ ~~$a^2+b^2 \mid x^2+y^2$~~

$a^2+b^2 \nmid ab$

∴ x^2+y^2 必有个大于1的正因子，其同时也为 a^2+b^2 的因子

∴ a^2+b^2 与 x^2+y^2 不互素、

8. 设 $n>1$，证明：$1+\frac{1}{2}+\cdots+\frac{1}{n}$ 不是整数.

证明：设 $t=[1,2,3,\cdots,n]$

∴ t 可表示作 $2^k\cdot m$，让 k 取得最大值，则 m 为奇数，且易知 $2^k \le n$

设 $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}=\frac{a}{t}$

∴ $a=t+\frac{t}{2}+\frac{t}{3}+\cdots+\frac{t}{n}$

∵ t 到 $\frac{t}{n}$ 之间，只有 $\frac{t}{2^k}$ 为奇，其余皆偶

∴ a 为奇数

又∵ t 为偶数

∴ $\frac{a}{t}$ 不可能为整数 ∴ 命题得证