整数的可除性

任课教师：胡丽琴
网络空间安全学院

RSA公钥密码系统

- 每个使用者产生各自的公钥K_e和私钥K_d.
- 随机产生两个不同的大素数p和q，二者具有相同的阶
- 计算$n=pq$和$\varphi(n)=(p-1)(q-1)$；
- 随机选取整数e，$1<e<\varphi(n)$，使得$(e,\varphi(n))=1$；
- 运用广义Euclid除法，计算唯一的整数d，$1<d<\varphi(n)$，使得

$$ed\equiv 1(\bmod\ \varphi(n))$$

- A的公钥是$K_e^A=(n,e)$，私钥是$K_d^A=d$。

RSA公钥密码系统

- 每个使用者产生各自的公钥K_e和私钥K_d.
- 随机产生两个不同的大素数p和q，二者具有相同的阶
- 计算$n=pq$和$\varphi(n)=(p-1)(q-1)$；
- 随机选取整数e，$1<e<\varphi(n)$，使得$(e,\varphi(n))=1$；
- 运用广义Euclid除法，计算唯一的整数d，$1<d<\varphi(n)$，使得

$$ed\equiv 1(\bmod\ \varphi(n))$$

- A的公钥是$K_e^A=(n,e)$，私钥是$K_d^A=d$。

整数的可除性

- 最大公因数
- (广义)Euclid除法
- Euler函数
- 同余

认识数论

- 数论是研究数的集合

- 整数集合{…,−3, −2, −1,0,1,2,3,…}中各种有意思的数
- 奇数、偶数
- 素数(质数)、合数
- 平方数(1,4,9,16,…)、立方数(1,8,27,64,…)
- 完全数(6,28,496,…)
- 斐波那契数(1,1,2,3,5,8,13,21,…)

认识数论

- ✓ Question1：3547898是不是平方数？
- ✓ Question2：9837856是不是平方数？

■ 平方数性质：

- ✓ 个位数为0,1,4,5,6,9
- ✓ 完全平方数的十位数字是奇数，则它的个位数字一定是6；反之，如果完全平方数的个位数字是6，则它的十位数字一定是奇数
- ✓ …………

整除的概念

整除

- 易判断：3整除6，5不整除76，7整除49，9不整除372…………

- 那么，具体是如何判断两个数之间是否有整除关系？有没有一个固定的准则来

整除的概念

整除

- **定义1.1.1** 设a, b是任意两个整数，其中$b \neq 0$。

  如果存在一个整数q，使得

  $$a = qb$$

  成立，则称b整除a或者a被b整除，记做$b \mid a$ 。

  此时q可以写成a / b或$\frac{a}{b}$。

- 如果$b \mid a$ ，则b叫做a的因数，a叫做b的倍数。

整除的概念

- 注：
  - 当b遍历整数a的所有因数时，$-b$也遍历整数a的所有因数；当b遍历a的所有因数时，a/b也遍历a的所有因数；
  - 0是任何非零整数的倍数；
  - 1是任何整数的因数；
  - 任何非零整数a是其自身的倍数，也是自身的因数。
- 例：试找出30的所有因数。

整除的概念

- 例：$7|84$，$84|336$，那么，7是否整除336？

- 例：$7|84$，$7|336$，那么，7是否整除336+84？7是否整除336-84？

- 例：$7|14$，$7|21$，那么，7是否整除$3\times21+4\times14$？7是否整除$587\times21+459\times14$？

整除的概念

- **性质1** 设$a, b\neq 0, c\neq 0$是三个整数。若$b|a$，$c|b$，则$c|a$.
- **性质2** 设$a, b, c\neq 0$是三个整数。若$c|a$，$c|b$，则$c|a\pm b$.
- **性质3**设$a, b, c\neq 0$是三个整数。若$c|a$，$c|b$，则对任意整数s,t，有$c|sa+tb$.

整除的概念

- 0~10中哪些是素数？哪些是合数？怎么判断的？

- **定义1.1.2** 设整数$n\neq 0, \pm 1$。如果除了自然的因数± 1和$\pm n$外，n没有其它因数，那么n叫做**素数**(或质数、不可约数)，否则n叫做**合数**。

- 当整数$n\neq 0, \pm 1$时，n和$-n$同为素数或合数。因此，**素数总是指正整数**，通常写成p。

整除的概念

- 一些特殊的素数：5, 7, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263
- 安全素数：奇素数p叫做安全素数，如果$(p-1)/2$也是素数

整除的概念

- 如何判断一个数是否为素数？比如：587是不是素数？9631是不是素数？
- **定理1.1.4** 设n是一个正合数，p是n的一个大于1的最小正因数，则p一定是素数，且$p\leq\sqrt{n}$
- **素数的判定**：设n是一个正整数，找出不大于$\sqrt{n}$的所有素数p，若存在素数p整除n，则n为合数，否则n为素数。

整除的概念

- 素数有多少个？有限多个？无穷多个？
  怎么判断的？有依据吗？

- 素数有无穷多个

整除的概念

- **例** 设$a, b, c\neq 0$是三个整数。若$c|a$，$c|b$，若存在整数s,t，使得

$$sa+tb=1,$$

则$c=?$

- 练习：设$a, b,$是两个非零整数，且有整数s,t，使得$sa+tb=1$。证明：若有$a|c$，$b|c$，则$ab|c$

●Euclid除法

- 设b=15，a=51，a是否被b整除？

- a不被b整除，那么a和b之间是什么关系？能不能用唯一的一个式子表达？

Euclid除法

- **定理1.2.1(Euclid除法)** 设a,b是两个整数，其中$b>0$，则存在唯一的整数q, r使得

$$a=qb+r,\ 0\le r<b. \qquad (2.1)$$

- **定义1.2.1** (2.1)式中的q叫做a被b除所得的**不完全商**，r叫做a被b除所得的**余数**。

●Euclid除法

- 推论 在定理1.2.1的条件下，$b|a$的充要条件是a被b除所得的余数$r=0$.

- **定义1.2.2** 设x是一个实数，称小于或等于x的最大整数为x的整数部分，记成$[x]$。这时，我们有

$$[x] \leq x < [x]+1.$$

●Euclid除法

注： 定理1.2.1中的不完全商q可以写成$q=[\frac{a}{b}]$，余数可以写成$r=a-qb=a-[\frac{a}{b}]b$。

- **例** 求[3.14]，[−3.14]。
- **定理1.2.2(Euclid除法)** 设a,b是两个整数，其中$b>0$，则对任意的整数c，存在唯一的整数q, r使得

$$a=qb+r,\ c\le r<c+b. \qquad (2.2)$$

●Euclid除法

- 实际运用Euclid除法时，常采用如下形式的余数
  - 当c=0时，$0\leq r<b$，这时r叫做**最小非负余数**。
  - 当c=1时，$1\leq r\leq b$，这时r叫做**最小正余数**。
  - 当c=$-b+1$时，$-b+1\leq r\leq 0$，这时r叫做**最大非正余数**。
  - 当c=$-b$时，$-b\leq r<0$，这时r叫做**最大负余数**。
  - 当$c=-[b/2]$或$-[b/2]+1$时，$-b/2\leq r<b/2$或$-b/2<r\leq b/2$，这时r叫做**绝对值最小余数**。

●Euclid除法

- **例** 将整数642表示为2进制形式。
- 运用Euclid除法，可以得到如下结论：
- **定理1.2.3** 设b是大于1的整数，则每个正整数n都可唯一的表示成

$$n=a_{k-1}b^{k-1}+a_{k-2}b^{k-2}+\ldots+a_1b+a_0,$$

其中a_i是整数，$0\le a_i\le b-1$，$i=0,\ldots,k-1$，且首项系数$a_{k-1}\neq 0$.

Euclid除法

- **定义1.2.3** 用$n=(a_{k-1}a_{k-2}\ldots a_1a_0)_b$表示展开式

$$n=a_{k-1}b^{k-1}+a_{k-2}b^{k-2}+\ldots+a_1b+a_0,$$

其中$0\leq a_i\leq b-1$，$i=0,\ldots,k-1$，$a_{k-1}\neq 0$，并称其为整数n的**b进制表示**。

- 这时，n的b进制位数是$k=[\log_b n]+1$.事实上，

$$b^{k-1}\leq n<b^k \text{ 或 } k-1\leq\log_b n<k.$$

因此，$k-1=[\log_b n]$。

●Euclid除法

当b=2时，系数a_i为0或1，因此我们有

- **推论** 每个正整数都可以表示成2的不同的幂之和
- 计算机也常用8进制、16进制等。在16进制中，我们用0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F分别表示0, 1, …, 15。
- **例1.2.6** 转换16进制$(ABC8)_{16}$为10进制。

●Euclid除法

- **例1.2.7** 转换16进制$(ABC8)_{16}$为2进制。

- **解**：$A=(1010)_2$, $B=(1011)_2$, $C=(1100)_2$, $8=(1000)_2$，

因此，

$$(ABC8)_{16}=(1010101111001000)_2.$$

- **例1.2.8** 转换2进制$(10111011111111101001)_2$为16进制.

最大公因数

- **定义1.3.1** 设$a_1,\ldots,a_n$是$n(n\geq 2)$个整数。若整数d是它们中每一个数的因数，那么d就叫做$a_1,\ldots,a_n$的一个**公因数**。

- d是$a_1,\ldots,a_n$的一个公因数的数学表达式为

$$d|a_1,\ \ldots,\ d|a_n.$$

最大公因数

- 如果整数$a_1,\ldots,a_n$不全为零，那么$a_1,\ldots,a_n$的所有公因数中最大的一个公因数叫做**最大公因数**，记做$\gcd(a_1,\ldots,a_n)$或$(a_1,\ldots,a_n)$。
- 特别地，当$(a_1,\ldots,a_n)=1$时，我们称$a_1,\ldots,a_n$**互素**或**互质**。

最大公因数

- **例1** 求21和35的所有公因数和最大公因数。
- **例2** 求21，35和-15的所有公因数和最大公因数。
- **例3** 求85和−391的所有公因数和最大公因数。
- 例：设a,b是两个正整数。如果$b|a$，则(a,b)=?
- 素数与任意整数之间有什么关系？

最大公因数

- 设p是一个素数，a为整数。证明：如果p不整除a，则p与a互素。

- $d>0$是$a_1,\ldots,a_n$的最大公因数的数学表达式为：
  - $d|a_1, \ldots, d|a_n$;
  - 若$e|a_1, \ldots, e|a_n$，则$e|d$.

- a,b的最大公因数$d=(a,b)$是集合$\{sa+tb|s,t\in \mathbf{Z}\}$中的最小正整数。

最大公因数

- 小学/中学学过的求最大公因数的方法是什么？
- 先用两个数公有的素因数连续去除，一直除到所得的商为互素的数为止，然后把所有的除数连乘起来，就得到两个数的最大公因数。
- 例 求下面两个整数的最大公因数：(1)25和35; (2)49和63

最大公因数

(1) $\begin{array}{r|rr} 5 & 25 & 35 \\ \hline & 5 & 7 \end{array}$

(2) $\begin{array}{r|rr} 7 & 49 & 63 \\ \hline & 7 & 9 \end{array}$

- 思考：除了这种方法有没有别的方法？
- 如何计算8251和6105的最大公因数？

最大公因数

- 例 求(87,6)=? (6,3)=?

  (173,15)=? (15,8)=?

  (145,20)=? (20,5)=?

- 这些数之间什么关系？说明什么？

- **定理1.3.3** 设a,b,c是三个不全为零的整数。如果

$$a=qb+c,$$

其中q是整数，则$(a,b)=(b,c)$.

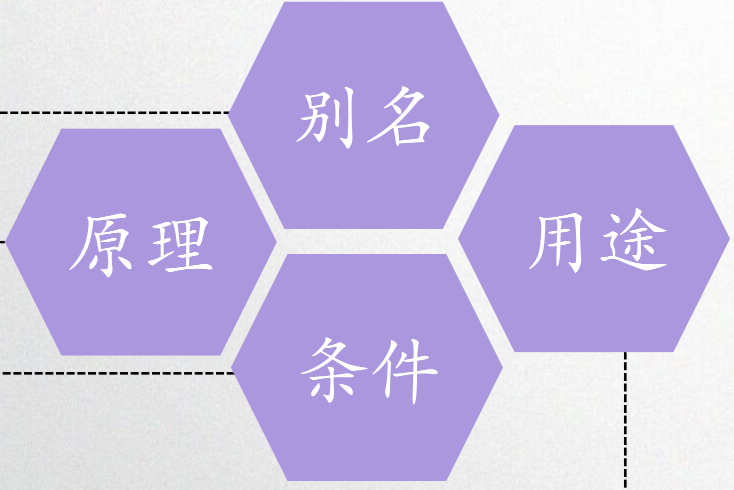
广义Euclid除法

辗转相除法

$\gcd(a,b) = \gcd(b, a-b)$

$a>b$且b不整除a

计算两个正整数a，b的最大公约数



广义Euclid除法

- 设a,b是任意两个正整数，记$r_{-2}=a, r_{-1}=b$，我们有

$$
\begin{aligned}
&r_{-2}=q_0r_{-1}+r_0, \quad 0\le r_0<r_{-1},\\
&r_{-1}=q_1r_0+r_1, \quad 0\le r_1<r_0,\\
&r_0=q_2r_1+r_2, \quad 0\le r_2<r_1,\\
&\vdots \\
&r_{n-3}=q_{n-1}r_{n-2}+r_{n-1}, \quad 0\le r_{n-1}<r_{n-2},\\
&r_{n-2}=q_nr_{n-1}+r_n, \quad 0\le r_n<r_{n-1},\\
&r_{n-1}=q_{n+1}r_n+r_{n+1}, \quad r_{n+1}=0.
\end{aligned}
\tag{3.1}
$$

广义Euclid除法

定理1.3.4

- 设a,b是任意两个正整数，则$(a,b)=r_n$，其中r_n是(3.1)中最后一个非零余数。

- 例 设$a=55$，$b=85$，计算(a,b)。

- 解： $85=1\times 55+30$,

  $55=1\times 30+25$,

  $30=1\times 25+5$,

  $25=5\times 5+0$.

所以，$(a,b)=5$.

●广义Euclid除法

从广义Euclid除法的运算过程中，我们有

$$
\begin{aligned}
r_n &= r_{n-2} - q_n r_{n-1}, \\
r_{n-1} &= r_{n-3} - q_{n-1} r_{n-2}, \\
r_{n-2} &= r_{n-4} - q_{n-2} r_{n-3}, \\
&\vdots \\
r_2 &= r_0 - q_2 r_1, \\
r_1 &= r_{-1} - q_1 r_0, \\
r_0 &= r_{-2} - q_0 r_{-1}.
\end{aligned}
\tag{3.1}
$$

逐次消去$r_{n-1}, r_{n-2}, \ldots, r_2, r_1, r_0$，可以找到整数$s, t$，使得$sa+tb=(a,b)$。

广义Euclid除法

例

- 设a=55，b=85，求整数s, t，使得 $sa+tb=(a,b)$。

- 解：$5=30-1\times25$

  $=30-1\times(55-30)$

  $=2\times30-55$

  $=2\times(85-55)-55$

  $=2\times85-3\times55$

所以，$s=-3, t=2$满足$sa+tb=(a,b)$。

●广义Euclid除法

- 下面的定理给出了s, t的具体计算方法。
- **定理1.3.5** 设a，b是任意两个正整数，则$s_n a+t_n b=(a,b)$，

对于j=0, 1, 2,…, n−1, n，这里s_j，t_j归纳地定义为

$$\begin{cases} s_{-2}=1, s_{-1}=0, s_j=s_{j-2}-q_j s_{j-1}, \\ t_{-2}=0, t_{-1}=1, t_j=t_{j-2}-q_j t_{j-1}, \end{cases} \qquad j=0,1,2,\Lambda\ ,n-1,n,$$

其中$q_j=[r_{j-2}/r_{j-1}]$是(3.1)式中的不完全商。

广义Euclid除法

- **定理1.4.1** 设n是一个正整数。如果对于所有的素数$p\le\sqrt{n}$，都有$p\nmid n$，则n一定是素数。

定理

- **证明：** 反证法。如果n是合数，则n有一个大于1的最小正因数p，即有$p|n$。根据定理1.1.4，p是素数，且$p\le\sqrt{n}$。这与假设条件矛盾，所以n是素数。

平凡除法

例： 求出所有不超过100的素数

对于任意给定的整数N，要求出所有不超过N的素数。

列出N个整数，从中删除小于等于$\sqrt{N}$的所有素数$p_1, p_2, \ldots, p_k$的倍数。

具体地是：依次删除

p_1的倍数：$2p_1, 3p_1, \ldots, [N/p_1]p_1$;

p_2的倍数：$2p_2, 3p_2, \ldots, [N/p_2]p_2$;

……

p_k的倍数：$2p_k, 3p_k, \ldots, [N/p_k]p_k$.

余下的大于1的整数就是所要求的不超过N的素数。

素数的生成

- 判断137是否为素数

例

- **解**：$11<\sqrt{137}<12$。小于12的所有素数为2,3,5,7,11，所以依次用2,3,5,7,11去试除137：

$137=68\times2+1$，$137=45\times3+2$，$137=27\times5+2$，

$137=19\times7+4$，$137=12\times11+5$.

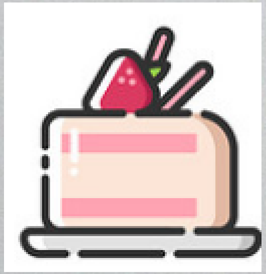
因此，$2\nmid137$，$3\nmid137$，$5\nmid137$，$7\nmid137$，$11\nmid137$。

根据定理1.4.1，$N=137$是素数。

最大公因数性质

- 例 计算42和90的所有公因数和最大公因数

性质1



- **定理1.5.1** 设a,b是任意两个不全为零的整数，d是正整数，则d是a,b的最大公因数的充要条件是：

1. $d|a$，$d|b$；
2. 若$e|a$，$e|b$，则$e|d$.

最大公因数性质

- **例1** 分别计算(18,22)，(9, 11)和(99, 121)。
- **例2** 计算(338,442)和(26,34)

性质2

- **定理1.5.2** 设a,b是任意两个不全为零的整数，

1. 若m是任意正整数，则$(am,bm)=(a,b)m$；
2. 若非零整数d满足$d|a$，$d|b$，则$(a/d,b/d)=(a,b)/d$。特别地，

$$(a/(a,b),b/(a,b))=1.$$

最大公因数性质

- 例 计算最大公因数(120,150, 210, 35).

性质3

- **定理1.5.3** 设$a_1,a_2,\ldots,a_n$是n个整数，且$a_1\neq 0$。令

$$(a_1,a_2)=d_2,\ (d_2,a_3)=d_3,\ \ldots,\ (d_{n-1},a_n)=d_n,$$

则$(a_1,a_2,\ldots,a_n)=d_n$.

*

最大公因数性质

性质4

- **例1** 计算(72,91)，(5, 91)和(360,91)。
- **例2** 计算(72,91)，(5, 91)和(360,91)。

- **定理1.5.6** 设$a_1, a_2, \ldots, a_n, c$是整数。如果对每个i，都有$(a_i, c)=1$，则

$$(a_1 a_2 \ldots a_n, c)=1.$$

- **推论** 设$a_1, a_2, \ldots, a_n$是n个整数，p是素数。如果$p|a_1 a_2 \ldots a_n$，则p一定整除某一个a_k。

最小公倍数

- **定义1.5.1** 设$a_1, a_2, \ldots, a_n$是n个整数。若m是这n个数的倍数，则m叫做这n个数的一个公倍数。$a_1, a_2, \ldots, a_n$的所有公倍数中的最小正整数叫做**最小公倍数**，记作$[a_1, a_2, \ldots, a_n]$.

- $m=[a_1, a_2, \ldots, a_n]$的数学表达式为
  - $a_1|m, \ldots, a_n|m$;
  - 若$a_i|m'$, $1\le i\le n$，则$m|m'$.

最小公倍数

- 例 设a=5，b=17，$[a,b]$=? (a,b)=?
- 例 设a=15，b=51，$[a,b]$=? (a,b)=?

例

- 设a=7，b=13，c=273，则a、b、c之间什么关系？ab与c是什么关系？

最小公倍数

- **定理1.5.7** 设a, b是两个互素的正整数。则
  - 若$a|m$, $b|m$，则$ab|m$;
  - $[a,b]=ab$.

- a, b是不是互素呢？

- **例** 设$a=6$，$b=15$，$c=150$，则ab与c之间还有没有整除关系？

最大公因数性质

性质

- **定理1.5.8** 设a，b是两个正整数，则
  - 若$a|m$, $b|m$，则$[a,b]|m$;
  - $[a,b]=ab/(a,b)$.

- **例** 计算最小公倍数[120,150,210,35]。

- **例** 计算[3,1989],[39,1989],[17,1989]，以及[[3×39×17],1989]

最大公因数性质

- **定理1.5.9** 设$a_1,a_2,\ldots,a_n$是n个整数。令

  $[a_1,a_2]=m_2$, $[m_2,a_3]=m_3$, …, $[m_{n-1},a_n]=m_n$,

  则$[a_1,a_2,\ldots,a_n]=m_n$.

性质

- **定理1.5.10** 设$a_1,a_2,\ldots,a_n$是正整数。如果

  $a_1|m$, …, $a_n|m$，则

$$[a_1,a_2,\ldots,a_n]|m.$$

算术基本定理

定理1.5.11(算术基本定理) 任一整数$n>1$都可以表示成素数的乘积，且在不考虑乘积顺序的情况下，该表达式是唯一的。即

$$n=p_1p_2\dots p_s,\ p_1\le p_2\le\dots\le p_s,$$

其中p_i是素数，并且若

$$n=q_1q_2\dots q_t,\ q_1\le q_2\le\dots\le q_t,$$

其中q_j是素数，则$s=t$，$p_i=q_j$，$1\le i\le s$.

标准分解式

- 分别写出整数45，68，289的因数分解式。

例

定理1.5.12 任一整数$n>1$都可以表示成

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s},\ \alpha_i>0,\ i=1,2,\dots,s, \tag{5.2}$$

其中$p_i<p_j\,(i<j)$是素数.

(5.2)式叫做整数n的**标准分解式**。

标准分解式

- **定理1.5.13** 设n是一个大于1的整数，且有标准分解式

$$n=p_1^{\alpha 1}p_2^{\alpha 2}\ldots p_s^{\alpha s},\ \alpha_i>0,\ i=1,2,\ldots,s,$$

则d是n的正因数当且仅当d有因数分解式

$$n=p_1^{\beta 1}p_2^{\beta 2}\ldots p_s^{\beta s},\ \alpha_i\geq\beta_i\geq 0,\ i=1,2,\ldots,s. \qquad (5.3)$$

标准分解式

- 求整数625和2154的标准分解式和全部因数。

例

- **解：** $625=5\times125=5^4$，$2154=2\times3\times359$

所以，625的所有因数为±1，±5，±25，±125，±625.

2154的所有因数为±1，±2，±3，±359，±6，±718，±1077，±2154.

- **例** 求整数45,68,289的最大公因数和最小公倍数。

● 标准分解式

- **定理1.5.14** 设a,b是两个正整数，且都有因数分解式

$$a=p_1^{\alpha 1}p_2^{\alpha 2}\dots p_s^{\alpha s},\ \alpha_i\geq 0,\ i=1,2,\dots,s,$$

$$b=p_1^{\beta 1}p_2^{\beta 2}\dots p_s^{\beta s},\ \beta_i\geq 0,\ i=1,2,\dots,s.$$

则a和b的最大公因数和最小公倍数分别有因数分解式

$$(a,b)=p_1^{\min(\alpha 1,\beta 1)}p_2^{\min(\alpha 2,\beta 2)}\dots p_s^{\min(\alpha s,\beta s)},$$

$$[a,b]=p_1^{\max(\alpha 1,\beta 1)}p_2^{\max(\alpha 2,\beta 2)}\dots p_s^{\max(\alpha s,\beta s)}.$$