**离散数学（二）--数论和密码学**

**整除**

* **定义1：a, b是整数，a ≠ 0，如果存在整数k使b = ak，则称a整除b，b能被a整除，记作a | b. 称b是倍数，a是 b的因数(因子).**
* 例：n, d是正整数，不超过n的正整数中有多少个能被d整除？
* 解：d的倍数可写作dk，1 ≤ dk ≤ n，则1/d ≤ k ≤ n/d, 1≤ k ≤ [n/d]. 有[n/d]个.
* **定理1：a, b, c是整数，a ≠ 0, b ≠ 0，则**
* **(i) a | b, a | c, 则a | (b + c);（可加性） (iv) 1 | c, a | 0;（1是任何整数的因数）**
* **(ii) b | c, 则ab | ac, b | ac;（可乘性） (v) a | b, 则 |a| ≤ |b|;**
* **(iii) a | b, b | c, 则a | c;（传递性） (vi) a | b, b | a, 则a = ±b.**
* 推论1 a, b, c, m, n是整数，a ≠ 0. 若a | b, a | c, 则 a | (mb + nc).（线性性）

**带余除法**（带余除法中余数不可为负）

* 定理2：a, b是整数，b > 0，则存在唯一的整数对q, r, 满足a = bq + r, 0 ≤ r < b.
* 证明：− |a| b ≤ − |a| ≤ a, 若bq ≤ a, 则q ≤ |q| ≤ b|q| ≤ |a|.
* 设q是使bq ≤ a的最大整数，则bq ≤ a < b(q+1), 0 ≤ r = a − bq < b. 至此证明了q, r的存在性。
* 若还有q1, r1满足a = bq1 + r1, 0 ≤ r1 < b，则：
* b (q − q1) + (r − r1) = 0, b|q − q1| = |r − r1| < b, 故 |q − q1| < 1. q = q1 , r = r1.

**最大公因数**

* **定义：a, b是整数，a、b至少有一个不为零，a, b公共的因数称为它们的公因数，公因数中最大的那个称为它们的最大公因数，记作gcd (a, b)或(a, b). 若(a, b) = 1，则称a, b互素。**
* **★引理：a = bq + r，则(a, b) = (b, r)**
* 证明：若k | a, k | b, 则k | (a − bq) = r；若k | b, k | r, 则k | (bq + r) = a. 故a, b和b, c有相同的公因数，从而有相同的最大公因数。
* **★定理：a, b是整数，a、b至少有一个不为零，则存在整数m, n使ma + nb = (a, b)**
* 证明：设k是形如ma + nb的最小正整数，k = m0a + n0b（m0，n0为整数且至少一个不为零）。用k除a有a = kq + r（0≤r＜k），将k带入有a = (m0a + n0b) q + r，故r = (1 - m0) a - n0qb，r也是形如ma + nb的正整数，又r＜k，故r = 0。因此a = kq，k | a，同理有k | b，因此k是a和b的公因数。若还有其它因数s满足s为a和b的公因数，由线性性可知s | m0a + n0b = k，故s≤| s |≤| k |≤k，因此k是所有a和b的公因数中的最大值。

**辗转相除法**

* a, b是整数，b > 0，a, b做带余除法，若余数不为零，用除数/余数分别作为下一次的被除数/除数，不断重复以上过程直到余数变为零。即：a = bq0 + r0, b = r0q1 + r1, r0 = r1q2 + r2, ……, rn−2 = rn−1qn−1 + rn.
* 其中b > r0 > r1 > r2 > ··· > rn = 0. 余数严格递减，有限项内必变为零。根据引理得：
* (a, b) = (b, r0) = (r0, r1) = ··· = (rn−2, rn−1) = (rn−1, rn) = rn−1. 即**最后一个非零余数**为a, b的最大公因数。
* 反向代入：rn−1 = rn−3 − rn−2qn−2 = rn−3 − (…)qn−2 = ··· = (…)a + (…)b
* 例：求(252, 198)，并将它表示为相应的的线性组合。
* 解：252 =1• 198 + 54 198 = 3 • 54 + 36 54 = 1 • 36 + 18 36 = 2 • 18 故(252, 198) = 18
* 反向求线性组合：18 = 54 − 1 • 36 = 54 − 1 • (198 − 3 • 54) = 4 • 54 − 1 • 198

= 4 • (252 − 1 • 198 ) − 1 • 198 = 4 • 252 − 5 • 198

**一些推论**

* **推论1：若k | a, k | b，则k | (a, b)**（证明：(a, b)可以写成ma+nb的形式，由线性性显然）
* **推论2：(ka, kb) = k(a, b)**
* **★推论3：a, b互素当且仅当存在整数m, n使ma + nb = 1**（充要条件）（证明：充分性同推论1；必要性：反证法，假设m, n有最大公因数k(k＞1），设m=pk, n=qk（p, q为互质的正整数）, 则ma+nb = apk+bqk = k(ap+bq) = 1，所以ap+bq = 1/k。因为a, b为自然数，p, q为正整数，所以ap+bq为整数，而1/k为分数，矛盾）
* **★推论4：若(a, b) = 1, a | bc, 则a | c**
* 证明：由(a, b) = 1知存在整数m, n使ma + nb = 1. 则c = (ma + nb)c = mac + nbc，再由 a | ac, a | bc可得a | c（因为mac + nbc是ac和bc的线性组合）.
* **推论5：若(a, b) = 1, a | c, b | c, 则ab | c**
* 证明：同上知存在整数m, n使ma + nb = 1. 则c = (ma + nb)c = mac + nbc，又由a | c, b | c知ab | bc, ab | ac，故mac + nbc是bc和ac的线性组合，由线性性得证。
* **推论6：若(a, b) = 1, (a, c) = 1, 则(a, bc) = 1**
* 证明：同上知存在整数m, n使ma + nb = 1，存在整数p, q使pa + qc = 1。带入得ma + (pa + qc) nb = 1，即(m + pnb) a + qnbc = 1，由线性性得证。

**素数**

* 定义1：p是正整数，p ≠ 1，若p的正因数只有1和p本身，则称p为素数。若p不是素数，则称p为合数。1既不是素数也不是合数。合数的相反数也称为合数。
* **定理：p是素数，p | ab，则p | a或p | b.**
* 证明：若p∤a, 则p, a的正共同因数只有1，故 (p, a) = 1. 由推论4可得p | b.
* **定理(整数的唯一分解性)：每个大于 1的整数都可写成素数之积，在不计次序的情况下写法唯一**
* **定理：存在无穷多个素数**

**整数的唯一分解性证明**

* 引理：大于1的整数必有素数因数。
* 证明：n = 2时命题成立。假设n < k时命题成立，当n = k时，若n为素数，命题成立；若n不为素数，n必有因数n1，1 < n1 < n, n1 < k, n1必有素因数，此素因数也是n的素因数。
* 存在性证明：n = 2时原命题成立。假设n < k时命题成立，当n = k时，若n为素数，命题成立；若n不为素数，n有素因数，取为p，1< n/p < k，由归纳假设得n/p可写成素数之积，从而n也可写成素数之积。
* 唯一性证明：n = 2时命题成立。假设n < k时命题成立，当n = k时，若n为素数，命题成立；若n不为素数，设n = p1p2 ··· ps = q1q2 ··· qt，p1 | p1p2 ··· ps = q1q2 ··· qt, 则p1整除某个qi. 不妨设p1 | q1, 但p1, q1均为素数，故p1 = q1. 1 < n/p1 <k, 由归纳假设得n/p1 = p2 ··· ps = q2 ··· qt的两式是同一分解，从而n的上两分解是相同的。
* 【欧拉对素数无穷性的证明】Σ 1/n = Σ 1/ppp = (1+1/p1+1/p12 + ···) (1+1/p2+1/p22 + ···) ··· = 1/ (1 − 1/p1)(1 − 1/p2) ··· 若素数个数有限，则上式收敛，但调和级数发散。实际上，Σ 1/n ~ ln n, Σ 1/p ~ lnln n.
* 定理：若，则
* 定义 a, b是非零整数，a, b的公共的倍数成为它们的公倍数，正公倍数中最小的那个称为它们的最小公倍数，记作lcm (a, b)或者 [a, b].
* 定理
* 推论1 (a, b)[a, b] = ab
* 推论2 则a, b互素
* 梅森数 Mp = 2p – 1, 费马数 , 641 | F5.

**欧拉函数**

* 定义 n是正整数，1-n中与n互素的数的个数记作φ(n).
* 定理 若 则φ(n) = n(1 − 1/p1)(1 − 1/p2) ··· (1 − 1/pt)
* 证明：令A = {1, 2, …, n}, Ai = {a ∈ A | pi | a}. 则Ai Aj = {a ∈ A | pipj | a}, Ai Aj Ak = {a ∈ A | pipjpk | a}, …
* N(Ai) = n / pi, N(Ai Aj) = n / pipj, …
* N(A1’ A2’ … At’) = n − Σ n/pi + Σ n/pipj + ···
* = n (1− Σ 1/pi + Σ 1/pipj + ···) = n(1 − 1/p1)(1 − 1/p2) ··· (1 − 1/pt)

**同余式**（注意这里的mod与作为运算符的 mod的区别）

* 定义3 m > 0, m | (a – b), 则称a, b关于模m同余，记作a ≡ b (mod m)
* 性质1 若a ≡ b (mod m), c ≡ d (mod m), 则
* (i) a + c ≡ b + d (mod m), ac ≡ bd (mod m); (ii) ka ≡ kb (mod m), ka ≡ kb (mod km);
* (iii) f(x)是整系数多项式，则 f(a) ≡ f(b) (mod m). (iv) (a, m) = (b, m).
* 性质2 ka ≡ kb (mod m), (k, m) = 1, 则a ≡ b (mod m)

**一次同余式**

* 性质3 若(a, m) = 1, 则存在b使 ab ≡ 1 (mod m).
* 证明：存在整数b, n使ab + nm = 1，两边取同余。

上面的b称为a模m的逆，它在同余的意义下唯一。

* 定理 若(a, m) = 1, 同余式 ax ≡ b (mod m) 有唯一解。
* 证明：存在c使ac ≡ 1 (mod m). acb ≡ b (mod m). x ≡ cb (mod m) 是原同余式的解。
* 若有两解x1, x2, 即ax1 ≡ b (mod m), ax2 ≡ b (mod m). ax1 ≡ ax2 (mod m), x1 ≡ x2 (mod m).
* 若d = (a, m) | b, 记a = da1, b = db1, m = dm1. 则同余式ax ≡ b (mod m)等价于a1x ≡ b1 (mod m1)
* 后式有唯一解，设为x ≡ x0 (mod m1) , 则x = x0 + m1 k, k = k1d, k1d + 1, …, k1d + d – 1. 换成同余式得
* x ≡ x0, x0 + m1, x0 + 2m1 …, x0 + (d – 1)m1 (mod m)
* 定理 同余式ax ≡ b (mod m) 有解的充要条件是(a, m) | b. 有解时恰好有d个解。
* 证明：充分性已证。必要性：若有解x, 则 ax – b = km, b = ax – km, (a, m) | b.

**模逆**

* 例：求4620模101的逆
* 4620 = 45 • 101 + 75 101 = 1 • 75 + 26 75 = 2 • 26 +23
* 26 = 1 • 23 + 3 23 = 7•3 + 2 3 = 1•2 + 1 2 = 2 •1
* 1 = 3 – 1•2 = 3 – 1 • (23 – 7 • 3) = – 1 • 23 + 8 • 3
* = – 1 • 23 + 8 • (26 – 1 • 23) = 8 • 26 – 9 • 23
* = 8 • 26 – 9 • (75 2 • 26 ) = – 9 • 75 + 26 • 26
* = – 9 • 75 + 26 • (101 – 1 • 75) = 26 • 101 – 35 • 75
* – 35 • 75 ≡ 1 (mod 101) , – 35 ≡ 66 (mod 101) . 故答案是66

**解一次同余式**

* 例：解同余式 111x ≡ 75 (mod 321)
* 解：321 = 2 • 111 + 99, 111 = 99 + 12, 99 = 8 • 12 + 3, 12 = 4 • 3.
* (111, 321) = 3 | 75.
* 3 = 99 – 8 • 12 = 99 – 8 • (111 – 99) = 9 • 99 – 8 • 111
* = 9 • (321 – 2 • 111) – 8 • 111 = 9 • 321 – 26 • 111
* – 26 • 111 ≡ 3 (mod 321), – 26 • 25 • 111 ≡ 75 (mod 321)
* 有解x ≡ – 26 • 25 ≡ 313 (mod 321)，全部解是x ≡ 99, 206, 313 (mod 321)

**欧拉定理**

* 定理 若(a, m) = 1, 则aφ(m) ≡ 1 (mod m)
* 证明：φ(m)表示1-m中与m互素的数的个数，将这些数记为b1, b2, …, bk. k = φ(m).
* abi与m互素；若bi ≢ bj (mod m), 则abi ≢ abj (mod m). 即abi 恰好与bj中的一个同余，故
* ab1 ab2 … abk ≡ b1 b2 … bk (mod m) ak b1 b2 … bk ≡ b1 b2 … bk (mod m)
* 由于b1 b2 … bk与m互素，故可将其消去。
* 费马小定理 若p是素数，p ∤ a, 则 ap–1 ≡ 1 (mod p)

**高次同余式**

* 高次同余式 xa ≡ b (mod m)
* 若b, m互素，则其解必与m互素。若还有a, φ(m)互素，则同余式ay ≡ 1 (mod φ(m))有解，取其解 c, 即
* ac ≡ 1 (mod φ(m)), ac = 1 + kφ(m), 将原同余式乘方c次，xac ≡ bc (mod m), x1+kφ(m) ≡ bc (mod m)
* 注意到xφ(m) ≡ 1 (mod m), 得到解x ≡ bc (mod m)
* 分析：上面关键是φ(m)，但是计算这个需要知道m的质因数分解；对于大整数，得到质因数分解很困难。
* 计算中也需要乘方运算，对于模乘方有下面的快速运算。

**模指数运算**

* 计算 3644 ≡ ? (mod 645)
* 解：645 = 3 • 215 = 3 • 5 • 43, φ(645) = (3 – 1)(5 – 1)(43 – 1) = 336
* 644 = 512 + 128 + 4
* 34 = 81, 38 = 812 = 6561 ≡ 111(mod 645),
* 316 = 1112 = 12321≡ 66 (mod 645), 332 ≡ 662 ≡ 486 (mod 645),
* 364 ≡ 4862 ≡ 126 (mod 645), 3128 ≡ 1262 ≡ 396 (mod 645),
* 3256 ≡ 3962 ≡ 81 (mod 645), 3512 ≡ 812 ≡ 111 (mod 645),
* 3644 ≡ 111 • 396 • 81 ≡ 36 (mod 645),

**RSA密码系统**

* 甲乙两人在公开的信道上进行通讯，由于信道公开，信息可能被偷听。下面考虑乙向甲传输信息的情况
* 1. 甲选择两个大素数p, q. 令n = pq, 再选择一数e与φ(n)互素，他将(n, e)传给乙。由于信道公开，(n, e) 也就公开了，称为公钥。
* 2. 乙将要传输的信息编码为与n互素的落于1-n中的整数，设为M，计算 Me ≡ C (mod n)，C同样落于 1-n中。乙将C传给甲。
* 3. 甲解同余式ed ≡ 1 (mod φ(n))算出d，即d满足ed = 1 + kφ(n). 则M ≡ M1+kφ(n) ≡ Mde ≡ Cd (mod n). d称为私钥。
* 分析：n, e公开，但至今很难将n分解为 pq, 也就得不到φ(n) , e也得不到，无法完成解密。
* 例 取p = 43, q = 59, e = 13. 则 n = 2537, 公钥是 (2537, 13).
* 对于明文M = 1819, 相应的密文是C ≡ 181913 ≡ 2081 (mod 2537).
* φ(2537) = (43 – 1)(59 – 1) = 2436.
* 解公钥是(2537, 13). 同余式13d ≡ 1 (mod 2436)，得d ≡ 937是与公钥是 (2537, 13) 配对的私钥。
* 对于密文C = 2081, 解密的方法是M ≡ 2081937 (mod 2537)

**数字签名**

* 甲要对文件进行签名，表明文件为他所发布。甲将一段信息用私钥进行加密附在文件的后面。
* 接收者乙用公钥对签名进行解密，得到有意义的信息，表明文件为甲发布。
* 这里只演示了公钥密码的基本原理。各个数要选的恰当，不致泄露n的分解式，也不能被别人猜到。

**密钥交换**

* 甲乙要商定一数字串作为通常的密码。甲乙要商定一个大素数p和正整数m < p.
* 甲想一个数a, 将A = ma mod p传给乙；乙想一个数b, 将A = mb mod p传给甲；
* Ab ≡ Ba ≡ mab (mod p) 即为所商定的数字串
* 分析：这里p, m公开，a, b不公开。知道A，要得到a要解mx ≡ (mod p), 同余式的指数方程对于很大的p, 即使是素数都很难。x称为离散对数。