为前程添彩！

我能过软考

利用扩展欧几里德算法求乘法逆元

主要内容

我能过软考

- ✓利用扩展欧几里德算法求乘法逆元

模n乘法逆元

对于整数a、 n，如果存在整数b，满足ab mod n =1，则说，b是a的模n乘法逆元。

定理：a存在模n的乘法逆元的充要条件是gcd(a,n) = 1

1）(X1,X2,X3) ←(1,0,n)；(Y1,Y2,Y3)←(0,1,a)

2）如果Y3=0返回X3=gcd(a,n)；无逆元
3）如果Y3=1返回Y3=gcd(a,n)；$Y2=a^{-1} \bmod n$
4）Q=max_int(X3/Y3)
5）(T1,T2,T3) ←(X1-Q·Y1,X2-Q·Y2,X3-Q·Y3)
6）(X1,X2,X3) ←(Y1,Y2,Y3)
7）(Y1,Y2,Y3) ←(T1,T2,T3)
8）回到 2）

求：67 mod 119的逆元

求解过程

Q	X1	X2	X3	Y1（T1）	Y2（T2）	Y3（T3）
-	1	0	119	0	1	67
1	0	1	67	1	-1	52
1	1	-1	52	-1	2	15
3	-1	2	15	4	-7	7
2	4	-7	7	-9	16	1

Q=1　T1=X1-Q*Y1=1　T2=X2-Q*Y2=-1　T3= X3-Q*Y3=52

Q=1　T1=0-1=-1　T2=1+1=2　T3=67-52=15

Q=3　T1=1+3=4　T2=-1-6=-7　T3=52-45=7

Q=2　T1=-1-8=-9　T2=2+14=16　T3=15-2*7=1

67 mod 119的逆元是（ ）。
A．52　B．67　　C．16　　D．19

A、67*52-1=3483
3483/119=29.26

B、67*67-1=4488
4488/119=37.71

C、67*16-1=1071
1071/119=9

D、67*19-1=1272
4488/119=10.69

参考答案：C

谢谢！

我能过软考

523124613