教育課題演習　第 13 回　フェルマーの小定理

１．一次不定方程式 $ax+by=1$

a と b が互いに素であるとき，方程式 $ax+by=1$ は整数の解を持つ。

（a,b の最大公約数が 1 であるとき，　a と b が互いに素であるという。）

２．整数の合同式

m を 1 より大きい整数とする。

整数 a を m で割った余りを　$a \bmod m$　で表す。

2 整数 a，b に対し，$a \bmod m = b \bmod m$　であることを，$a \equiv b \pmod m$　で表す。

合同式の基本性質

$a \equiv b \pmod m$ ⇔ $a-b$ は m の倍数

$a \equiv b \pmod m$ ⇔ $a+c \equiv b+c \pmod m$

$a \equiv b \pmod m$ ⇒ $ac \equiv bc \pmod m$

a と m が互いに素であるとき，方程式 $ax \equiv 1 \pmod m$ を満たす整数 x が存在する。

c と m が互いに素であるとき，$a \equiv b \pmod m$ ⇔ $ac \equiv bc \pmod m$

特に，p が素数であれば,

$0<a<p$　のとき，方程式 $ax \equiv 1 \pmod p$ を満たす整数 x が存在する。

$0<c<p$　のとき，　$a \equiv b \pmod p$ ⇔ $ac \equiv bc \pmod p$

２．素数を法とする剰余系における乗算と累乗

例　7 を法とする剰余系における乗算

$ab \bmod 7$

a \ b	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

素数を法とする剰余系における累乗

$a^k \bmod 7$

a \ k	1	2	3	4	5	6
1	1					
2	2					
3	3					
4	4					
5	5					
6	6					

３．２項定理

$(a+b)^n=a^n+{}_nC_1a^{n-1}b++{}_nC_2a^{n-2}b^2+\cdots\cdots+{}_nC_{n-2}a^{n-2}b^2+{}_nC_{n-1}ab^{n-1}+b^n$

$a=b=1$，$n=p$ とおくと，

$2^p=1+{}_pC_1+{}_pC_2+\cdots\cdots+{}_pC_{p-2}+{}_pC_{p-1}+1$

${}_pC_k=\dfrac{p!}{k!(p-k)!}$ なので，

p が素数のとき，${}_pC_1, {}_pC_2$，…，${}_pC_{p-2}$，${}_pC_{p-1}$ は p の倍数。

∴　$2^p\equiv 2 \pmod p$

∴　$2^{p-1}\equiv 1 \pmod p$