4.3 The theorem of Fermat and Wilson revisited

June 21, 2016

3

a)

1. $(a, m) = 1$
2. $(a - 1, m) = 1$

$\diamond$ $1 + a + a^2 + \cdots + a^{\phi(m)-1} \equiv 0(\textbf{mod } m)$

Car on a que $\sum_{j=0}^{\phi(m)-1} a^j = \frac{1 - a^{\phi(m)}}{1 - a}$.

Donc $(a-1)\sum_{j=0}^{\phi(m)-1} a^j = a^{\phi(m)} - 1$. Or, par le théorème d'Euler, on a que $a^{\phi(m)} - 1 \equiv 0(\text{mod } m)$. Donc $(a-1)\sum_{j=0}^{\phi(m)-1} a^j \equiv 0(\text{mod } m)$. Puisque $(a-1, m) = 1$, on peut retirer le terme $(a-1)$ et alors on a le résultat voulu.

4*

1. $r_1, \cdots, r_{\phi(m)}$ un système de résidue réduit
2. m impair

$\diamond$ $r_1 + r_2 + \cdots + r_{\phi(m)} \equiv 0(\textbf{mod } m)$

Puisque m est impair, on a que pgdc$(m, 2) = 1$ et donc $2r_i$ possède un résidue unique dans le système puisqu'il s'agit d'un nombre relativement premier à m. Il en va de même pour chaque $2r_j$ auquel correspond un unique résidue.

Ansi, on a que $2\sum_{j=1}^{\phi(m)} r_j \equiv \sum_{j=1}^{\phi(m)} r_j(\text{mod } m)$ et donc $\sum_{j=1}^{\phi(m)} r_j \equiv 0(\text{mod } m)$.

11

1. p premier et différent de 2
2. $0 \leq a \leq p-1$

$\diamond$ $\binom{p-1}{a} \equiv (-1)^a (\mathbf{mod}\ p)$

La chose est évidente pour $\binom{p-1}{0}$ et $\binom{p-1}{p-1}$. Supposons la chose vraie pour $a-1$ et considérons $0 < a < p-1$.

On a

$$\binom{p-1}{a} - (-1)^a = \binom{p-1}{a-1}\frac{p-1}{a} - (-1)^a$$
$$=$$
$$\frac{\binom{p-1}{a-1}p - \binom{p-1}{a-1}a - (-1)^a a}{a}$$
$$=$$
$$\binom{p-1}{a-1}\frac{p}{a} - \left[\binom{p-1}{a-1} + (-1)^a\right]$$
$$=$$
$$\binom{p}{a} + \left[\binom{p-1}{a-1} - (-1)^{a-1}\right]$$

Or, on a que $\binom{p}{a}$ est divisible par p (**ex. 3-1 9 et** $0 < a < p-1$) et $\binom{p-1}{a-1} - (-1)^{a-1}$ l'est également par hypothèse d'induction.

12

1. $n < p \leq 2n$
2. p premier

$\diamond$ p **divise** $\binom{2n}{n}$ **mais pas** p^2

On a que $\binom{2n}{n} = p\frac{2n\cdots(p+1)(p-1)\cdots(n+1)}{n!} = d$ et donc $2n\cdots(p+1)(p-1)\cdots(n+1) = \frac{n!d}{p}$, d'où l'on conclut que $\frac{n!d}{p}$ est un entier et donc p divise $n!d$.

Or $p \nmid n, (n-1), \cdots 2$ puisque p est premier. Donc p divise d par **cor. 2-3**. Alors $\frac{2n\cdots(p+1)(p-1)\cdots(n+1)}{n!} = \frac{d}{p}$ un entier. Mais alors $\binom{2n}{n} = p\frac{2n\cdots(p+1)(p-1)\cdots(n+1)}{n!} = pk$ où k est un entier. Donc $p \mid \binom{2n}{n}$.

Supposons alors que p^2 divise $\binom{2n}{n}$. On a que $kp^2 = \frac{2n!}{(n!)^2} \Leftrightarrow lp^2 = 2n!$ pour un certain k. Donc $p^2 \mid 2n!$.

Alors $lp = 2n\cdots(p+1)(p-1)! = 2n\cdots(p+1)(p\alpha - 1)$ pour un certain entier α par **thm. 5-3**. Or $p \nmid (p\alpha - 1)$. De plus $n < p < 2n < 2p$. Or, par

cor. 2-3 et cor. 2-4, p doit diviser $p+1$ ou $p+2$ ou ... $2n$, ce qui est impossible.

14

◇ **Calculer la quantité de nombre premier comprise dans l'interval fermé** $[m!+2, m!+m]$ **où** $m > 1$

Soit $0 \leq k \leq m-2$. Alors on a que $m!+2 \leq m!+2+k \leq m!+m$. Or, on a que $m!+2+k = m!+q = m \cdots q!+q$ et donc pour tout $q = 2+k$, on a que $m!+2+k$ est divisible par q. Or, $q < m!+q$ et donc $m!+q = dq$ où $d > 1$. Donc $m!+q$ n'est pas premier et ce pour tout k entre 0 et $m-2$.