UNIVERSITÉ DE RENNES 1

Théorie des nombres

Interrogation 1 : corrigé

Exercice 1

Trouver tous les générateurs de $\mathbb{F}_{11}^\times$.

Le groupe $\mathbb{F}_{11}^\times$ est isomorphe à $\mathbb{Z}/10\mathbb{Z}$. Il a donc $\phi(10) = (2-1)(5-1) = 4$ générateurs.

On a $2^2 \equiv 4 \not\equiv 1 \pmod{11}$ donc l'ordre de 2 dans $\mathbb{F}_{11}^\times$ ne divise pas 2.

On a $2^4 \equiv 16 \equiv 5 \pmod{11}$, donc $2^5 \equiv 10 \equiv -1 \not\equiv 1 \pmod{11}$, donc l'ordre de 2 dans $\mathbb{F}_{11}^\times$ ne divise pas 5.

L'ordre de 2 dans $\mathbb{F}_{11}^\times$ est donc un diviseur de 10 qui n'est ni un diviseur de 2 ni un diviseur de 5, donc c'est 10. Donc 2 est un générateur de $\mathbb{F}_{11}^\times$.

L'application $m \mapsto 2^m$ donne alors un isomorphisme de $\mathbb{Z}/10\mathbb{Z}$ sur $\mathbb{F}_{11}^\times$. Or, les 4 générateurs de $\mathbb{Z}/10\mathbb{Z}$ sont 1, 3, 7 et 9 (i.e. les entiers premiers à 10 entre 0 et 9). Par l'isomorphisme précédent, on en déduit que les générateurs de $\mathbb{F}_{11}^\times$ sont 2, $2^3 \equiv 8$, $2^7 \equiv 7$ et $2^9 \equiv 6$.

Les générateurs de $\mathbb{F}_{11}^\times$ sont donc 2, 6, 7 et 8.

Exercice 2

Calculer les symboles de Jacobi suivants. (Chaque étape du calcul devra être justifiée).

$\left(\frac{58}{77}\right)$

$$
\begin{aligned}
\left(\frac{58}{77}\right) &= \left(\frac{2}{77}\right)\left(\frac{29}{77}\right) && \text{car } 58 = 2 \cdot 29 \\
&= -\left(\frac{29}{77}\right) && \text{car } 77 \equiv -3 \pmod 8 \\
&= -\left(\frac{77}{29}\right) && \text{car } 29 \equiv 1 \pmod 4 \\
&= -\left(\frac{19}{29}\right) && \text{car } 77 \equiv 19 \pmod{29} \\
&= -\left(\frac{29}{19}\right) && \text{car } 29 \equiv 1 \pmod 4 \\
&= -\left(\frac{10}{19}\right) && \text{car } 29 \equiv 10 \pmod{19} \\
&= -\left(\frac{2}{19}\right)\left(\frac{5}{19}\right) && \text{car } 10 = 2 \cdot 5 \\
&= \left(\frac{5}{19}\right) && \text{car } 19 \equiv 3 \pmod 8 \\
&= \left(\frac{19}{5}\right) && \text{car } 5 \equiv 1 \pmod 4 \\
&= \left(\frac{4}{5}\right) && \text{car } 19 \equiv 4 \pmod 5 \\
&= 1 && \text{car } 4 = 2^2 \text{ et } \operatorname{pgcd}(4,5) = 1.
\end{aligned}
$$

$\left(\frac{19}{41}\right)$

$$
\begin{aligned}
\left(\frac{19}{41}\right) &= \left(\frac{41}{19}\right) && \text{car } 41 \equiv 1 \pmod 4 \\
&= \left(\frac{3}{19}\right) && \text{car } 41 \equiv 3 \pmod{19} \\
&= -\left(\frac{19}{3}\right) && \text{car } 19 \equiv 3 \equiv -1 \pmod 4 \\
&= -\left(\frac{1}{3}\right) && \text{car } 19 \equiv 1 \pmod 3 \\
&= -1.
\end{aligned}
$$

$\left(\frac{77}{91}\right)$

$$\begin{aligned}
\left(\frac{77}{91}\right) &= \left(\frac{91}{77}\right) && \text{car } 77 \equiv 1 \pmod 4 \\
&= \left(\frac{14}{77}\right) && \text{car } 91 \equiv 14 \pmod{77} \\
&= \left(\frac{2}{77}\right)\left(\frac{7}{77}\right) && \text{car } 14 = 2 \cdot 7 \\
&= 0 && \text{car } 7 \mid 77.
\end{aligned}$$

$\left(\frac{28}{59}\right)$

$$\begin{aligned}
\left(\frac{28}{59}\right) &= \left(\frac{2}{59}\right)^2\left(\frac{7}{59}\right) && \text{car } 28 = 2^2 \cdot 7 \\
&= \left(\frac{7}{59}\right) \\
&= -\left(\frac{59}{7}\right) && \text{car } 59 \equiv 7 \equiv -1 \pmod 4 \\
&= -\left(\frac{3}{7}\right) && \text{car } 59 \equiv 3 \pmod 7 \\
&= \left(\frac{7}{3}\right) && \text{car } 7 \equiv 3 \equiv -1 \pmod 4 \\
&= \left(\frac{1}{3}\right) && \text{car } 7 \equiv 1 \pmod 3 \\
&= 1.
\end{aligned}$$

Exercice 3

Question 1

Soient p un nombre premier impair et un entier $n \geqslant 1$. Soit $a \in \mathbb{Z}$ un entier premier à p. On suppose qu'il existe un entier x tel que $x^2 \equiv a \pmod{p^n}$. Montrer qu'il existe un $u \in \mathbb{Z}$ tel que $(x + p^n u)^2 \equiv a \pmod{p^{n+1}}$.

On cherche un entier u tel que

$$(x + p^n u)^2 \equiv a \pmod{p^{n+1}},$$

c'est-à-dire

$$x^2 + 2xp^n u + p^{2n} u^2 \equiv a \pmod{p^{n+1}}.$$

Comme $n \geqslant 1$, on a $p^{2n} u^2 \equiv 0 \pmod{p^{n+1}}$, donc on est ramené à

$$2xp^n u \equiv a - x^2 \pmod{p^{n+1}}.$$

Comme $x^2 \equiv a \pmod{p^n}$, on peut diviser par p^n, et l'on est ramené à

$$2xu \equiv \frac{a - x^2}{p^n} \pmod{p}.$$

Il suffit donc de montrer que $2x$ est inversible modulo p.

Comme p est impair, on a $2 \in (\mathbb{Z}/p\mathbb{Z})^\times$. Si x n'était pas inversible, on aurait $x \equiv 0 \pmod{p}$, donc $a \equiv 0 \pmod{p}$, et a ne serait pas premier à p.

Il existe donc un $u \in \mathbb{Z}$ tel que $(x + p^n u)^2 \equiv a \pmod{p^{n+1}}$.

Question 2

En déduire que a est un carré modulo p^n si et seulement si $\left(\frac{a}{p}\right) = 1$.

Si $\left(\frac{a}{p}\right) = 1$, alors il existe un entier x tel que $x^2 \equiv a \pmod{p}$, et a est premier à p. D'après la question précédente, on en déduit par récurrence que pour tout entier $k > 0$, il existe un entier x_k tel que $x_k^2 \equiv a \pmod{p^k}$. En particulier, a est un carré modulo p^n.

Réciproquement, si a est un carré modulo p^n, alors a est un carré modulo p, donc $\left(\frac{a}{p}\right) = 1$ puisque a est premier à p.

Question 3

Montrer de même que si a est un entier impair et si $n \geqslant 3$, alors a est un carré modulo 2^n si et seulement si $a \equiv 1 \pmod{8}$. (Indication : on pourra chercher u tel que $(x+2^{n-1}u)^2 \equiv a \pmod{2^{n+1}}$).

Si a est un carré modulo 2^n, alors c'est un carré modulo 8 (puisque $n \geqslant 3$), or les carrés dans $\mathbb{Z}/8\mathbb{Z}$ sont 0, 1 et 4. Comme a est impair, on a donc $a \equiv 1 \pmod 8$.

Réciproquement, supposons $a \equiv 1 \pmod 8$. Montrons par récurrence sur k la propriété suivante :
pour tout entier $k \geqslant 3$, il existe un entier x_k tel que $x_k^2 \equiv a \pmod{2^k}$.

Pour $k = 3$, $x_3 = 1$ convient.

Si, pour un certain entier $k \geqslant 3$, il existe un entier x_k tel que $x_k^2 \equiv a \pmod{2^k}$, montrons qu'il existe un entier u tel que $x_{k+1} = x_k + 2^{k-1}u$ vérifie $x_{k+1}^2 \equiv a \pmod{2^{k+1}}$, c'est-à-dire

$$x_k^2 + 2^k x_k u + 2^{2k-2}u^2 \equiv a \pmod{2^{k+1}}.$$

Comme $k \geqslant 3$, on a $2^{2k-2}u^2 \equiv 0 \pmod{2^{k+1}}$, donc cela équivaut à

$$2^k x_k u \equiv a - x_k^2 \pmod{2^{k+1}},$$

i.e. à

$$x_k u \equiv \frac{a - x_k^2}{2^k} \pmod 2.$$

Comme $x_k^2 \equiv a \equiv 1 \pmod 2$, on a $x_k \equiv 1 \pmod 2$, donc $u = \frac{a-x_k^2}{2^k}$ convient.

Question 4

Soit $N \geqslant 1$ un entier, et soit a un entier premier à N. Notons $N = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ la décomposition de N en produit de facteurs premiers, avec $p_1 < \dots < p_m$ premiers et des entiers $\alpha_1, \dots, \alpha_m > 0$. Montrer que les deux propriétés suivantes sont équivalentes :

(i) a est un carré modulo N ;

(ii) pour tout $i \in \{1, \dots, m\}$,

$$\begin{cases} a \equiv 1 \pmod 4 & \text{si } p_i = 2 \text{ et } \alpha_i = 2 \\ a \equiv 1 \pmod 8 & \text{si } p_i = 2 \text{ et } \alpha_i \geqslant 3 \\ \left(\frac{a}{p_i}\right) = 1 & \text{si } p_i > 2. \end{cases}$$

Si a est un carré modulo N, alors c'est un carré modulo p_i^r, pour tout $i \in \{1, \dots, m\}$ et tout $r \leqslant \alpha_i$. En particulier :

- si $p_i = 2$ et $\alpha_i = 2$, alors a est un carré dans $\mathbb{Z}/4\mathbb{Z}$, donc $a \equiv 0$ ou $1 \pmod 4$, donc $a \equiv 1 \pmod 4$ puisque $p_i \nmid a$;
- si $p_i = 2$ et $\alpha_i \geqslant 3$, alors a est un carré dans $\mathbb{Z}/8\mathbb{Z}$, donc $a \equiv 0, 1$ ou $4 \pmod 8$, donc $a \equiv 1 \pmod 8$ puisque $p_i \nmid a$;
- si $p_i > 2$, alors a est un carré dans $\mathbb{F}_{p_i}^\times$, donc $\left(\frac{a}{p_i}\right) = 1$.

Réciproquement, si la propriété (ii) est vérifiée, alors a est un carré modulo $p_i^{\alpha_i}$ d'après les questions 2 et 3, pour tout $i \in \{1, \dots, m\}$, donc a est un carré modulo N par le théorème chinois.