MPRI – cours 2.12.2

F. Morain

Préparation du TD du 2010/10/26

1. Trouver un multiple de 49 dont tous les chiffres décimaux sont égaux à 1.

2. Quels sont les générateurs de $(\mathbb{Z}/13\mathbb{Z})^*$?

3. Calculer $1/5 \bmod 17$.

4. (a) Montrer que si N est sans facteur carré, on a $a^{\lambda(N)+1} \equiv a \bmod N$ pour *tout* $a \in \mathbb{Z}/N\mathbb{Z}$.

(b) RSA: soit $N = pq$ avec p et q des nombres premiers distincts. Soit e tel que $\gcd(e, \lambda(N)) = 1$. On pose $d = 1/e \bmod \lambda(N)$. On chiffre $x \in \mathbb{Z}/N\mathbb{Z}$ par $E(x) = x^e \bmod N$. Montrer que E est inversible et donner son inverse.

(c) Calculer le nombre de points fixes de E, c'est-à-dire le nombre de x non chiffrés : $E(x) = x$.

5. Démontrer le théorème de Pocklington.

6. Prouver que si $N = \prod_i p_i^{\alpha_i}$, alors $P(N) = \prod_i \mathrm{pgcd}(p_i - 1, N - 1)$.

7. Trouver une famille d'entiers composés N vérifiant $F(N) = \varphi(N)/4$.

8. Montrer que N est premier si et seulement si $\varphi(N) \mid N - 1$.

9. Soit f un polynôme à coefficients entiers. Montrer comment trouver toutes les valeurs de $f(x)$ $\{p_1, p_2, \ldots, p_k\}$-friables de l'intervalle $[0, X]$ à l'aide d'un crible.

10. On suppose qu'on doit calculer le logarithme discret de $(a_i)_{1 \le i \le r}$ dans $G = \langle g \rangle$. Comment modifier l'algorithme des pas de bébé et des pas de géant pour optimiser le calcul de ces logarithmes ? Même question avec la méthode ρ de Pollard.

11. Montrer que si $p \equiv 2 \bmod 3$, alors le nombre de points sur $E : Y^2 = X^3 + 1$ est $p + 1$.

12. Soit E la courbe elliptique d'équation $y^2 = x^3 + x + 1$ définie sur $\mathbb{F}_5$. Trouver tous les points de cette courbe et en déduire la structure du groupe $E(\mathbb{F}_5)$.

13. Soit E une courbe elliptique définie sur $\mathbb{F}_p$, avec p premier. Soit $m = \#E(\mathbb{F}_p)$ son cardinal. Soit M un point sur E d'ordre ω. Montrer que si $p \ge 37$ et $(\sqrt{p} - 1)^2 \le \omega \le (\sqrt{p} + 1)^2$, alors $m = \omega$.

14. (a) Montrer qu'on peut évaluer $[15]P$ rapidement sur une courbe elliptique en calculant $[15]P = [16]P \ominus P$. Combien d'opérations aurait-on fait à l'aide de la méthode binaire classique ?

(b) Soit n un entier impair et k le plus grand entier tel que $n = n_1 2^k + (2^k - 1)$. Écrire une fonction de calcul de $[n]P$ utilisant cette dcomposition.

15. [Reconstruction rationnelle] Soit $m > t \ge 1$ des entiers et k un nombre réel vérifiant $1 \leqslant k \leqslant m$. Montrer qu'il existe deux entiers x et y tels que

$$yt \equiv x \bmod m, \text{ avec } |x| < k, 1 \leqslant y \leqslant \frac{m}{k}.$$