Teoria Elementare dei Numeri 2018 Appello 1 25 gennaio 2019, ore 10:00–12:00.

COGNOME ..... *NOME* .....

Inserire le risposte negli spazi predisposti, accompagnandole con *spiegazioni chiare e sintetiche.*
NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 6 punti.

1. *Sia φ la funzione di Eulero. Sia n un numero naturale e sia p un primo con la proprietà che p divide n, ma p^2 non divide n.*
   (a) Verificare che $\varphi(p)$ divide $\varphi(n)$;
   (b) Verificare che $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$.

Sol.: Se p divide n, ma p^2 non divide n, allora

$$n = p \cdot m, \qquad \text{con } m = \tfrac{n}{p} \text{ e } \gcd(p, m) = 1.$$

Ne segue che

$$\varphi(n) = \varphi(p) \cdot \varphi(m) = \varphi(p)\varphi(\frac{n}{p}),$$

e chiaramente $\varphi(p)$ divide $\varphi(n)$.

2. *(a) Determinare la più piccola radice primitiva $\bar{g}$ di $\mathbf{Z}_{31}$.*
   (b) Quante radici primitive ci sono in $\mathbf{Z}_{31}$?
   (c) Calcolare $\log_{\bar{g}} \overline{20}$, dove $\bar{g}$ è la radice primitiva ottenuta in (a).

Sol.: (a) Poiché $2^{15} \equiv 1 \mod 31$, abbiamo $a = 2$ non è una radice primitiva di $\mathbf{Z}_{31}$. Proviamo con $a = 3$: poiché modulo 31

$$3^{15} \equiv 30, \quad 3^{10} \equiv 25, \quad 3^6 \equiv 16,$$

$a = 3$ è la più piccola radice primitiva di $\mathbf{Z}_{31}$.

(b) In $\mathbf{Z}_{31}^*$ ci sono $\varphi(30) = \varphi(2)\varphi(3)\varphi(5) = 8$ radici primitive.

(c) Abbiamo

$$\log 20 = 2\log 2 + \log 5.$$

Cominciamo con i logaritmi noti in base 3:

$$\log_3 3 \equiv 1, \quad \log_3(-1) \equiv 15, \quad \log_3 1 \equiv 0 \mod 30.$$

Dalle relazioni modulo 31

$-1 \equiv 30 = 2 \cdot 3 \cdot 5$
$5 \equiv 36 = 2^2 \cdot 3^2$
$-1 \cdot 3 \equiv 2^2 \cdot 7$
$-1 \cdot 2 \cdot 5 \equiv 21 = 3 \cdot 7$

otteniamo le relazioni modulo 30 fra i rispettivi logaritmi in base 3:

$15 = \log 2 + 1 + \log 5$
$\log 5 = 2\log 2 + 2$
$15 + 1 = 2\log 2 + \log 7$
$15 + \log 2 + \log 5 = 1 + \log 7$

da cui

$\log 2 + \log 5 = 14$
$2\log 2 - \log 5 = -2$
$2\log 2 + \log 7 = 16$
$\log 2 + \log 5 - \log 7 = -14.$

Da qui si ricavano, modulo 30,

$$\log 7 = 28, \quad 2\log 2 = 18, \quad \log 5 = 20, \quad \log 2 = 24$$
$$\log 20 = 8.$$

3. *Sia E la curva di equazione $Y^2 = X^3 + X + 4$ su $\mathbf{Z}_5$.*
   (a) Verificare che si tratta di una curva ellittica.
   (b) Determinare tutti i punti di $E(\mathbf{Z}_5)$.
   (b) Esibire un punto di ordine massimo in $E(\mathbf{Z}_5)$.

Sol.: (a) Il discriminante della curva è $\Delta = 4 + 27 \cdot 16 \equiv 1 \not\equiv 0 \mod 5$. Dunque E definisce una curva ellittica su $\mathbf{Z}_5$.
(b) La curva $E(\mathbf{Z}_5)$ ha 9 punti

$$(0,2), \quad (0,3), \quad (1,1,), \quad (1,5), \quad (2,2), \quad (2,3), \quad (3,2), \quad (3,3), \quad \infty.$$

(c) La curva ha 9 punti, per cui il gruppo è isomorfo a $\mathbf{Z}_3 \times \mathbf{Z}_3$ oppure è ciclico e isomorfo a $\mathbf{Z}_9$. Nel primo caso tutti i punti hanno ordine minore o uuae a 3, nel secondo ci sono punti con ordine maggiore di tre. Prendiamo ad esempio $P = (0,2)$: calcolando $2P$ troviamo $2P = (1,4)$. Poiche' $2P \neq -P$, abbiamo che $3P \neq \infty$ e dunque P ha ordine maggiore di 3. Conclusione: il gruppo $E(\mathbf{Z}_5)$ è ciclico di ordine 9.

4. *Sia E la curva di equazione $Y^2 = X^3 - X$ su $\mathbf{Z}_p$, con $p > 2$ primo.*
   (a) Verificare che si tratta di una curva ellittica.
   (b) Verificare che il gruppo $E(\mathbf{Z}_p)$ non è mai ciclico.

Sol.: (a) Per ogni primo p, il discriminante $\Delta = -4 \neq 0$ e dunque E definisce una curva ellittica su $\mathbf{Z}_p$.
(b) Per ogni primo $p > 2$ la curva $Y^2 = X^3 - X$ ha 3 punti di ordine due, ossia $(0,0)$, $(1,0)$ e $(-1,0)$. Per questo il gruppo $E(\mathbf{Z}_p)$ non può essere ciclico: in un gruppo ciclico c'è un solo punto di ordine due.

5. *Sia $n = 8909$ e siano date le seguenti congruenze modulo n:*

$$3596^2 \equiv 3^2 \cdot 11 \cdot 43, \quad 5597^2 \equiv 5 \cdot 11 \cdot 43, \quad 3944^2 \equiv 2 \cdot 11,$$
$$4582^2 \equiv 2^{10} \cdot 5, \quad 8674^2 = 7 \cdot 11 \cdot 23, \quad 6827^2 = 2 \cdot 3^2 \cdot 5^2 \cdot 11.$$

   Fra quali interi possiamo cercare potenziali fattori non banali di n? (è sufficiente impostare il calcolo e spiegare...)

Sol.: Moltiplicando fra loro la terza e la sesta relazione, otteniamo la relazione quadratica

$$(3944 \cdot 6827)^2 \equiv (2 \cdot 3 \cdot 5 \cdot 11)^2 \mod 8909.$$

Potenziali fattori di n sono $a + b$ ed $a - b$, con

$$a = 3944 \cdot 6827 \mod \text{n}, \qquad \text{b} = 2 \cdot 3 \cdot 5 \cdot 11 \mod \text{n}.$$

Nel nostro caso, $a = 2690$, $b = 330$ e

$$\gcd(a + b, n) = 151, \qquad \gcd(a - b, n) = 59.$$

la terza e la sesta.

Alternativamente, moltiplicando fra loro la prima, la seconda e la quarta relazione, otteniamo la relazione quadratica

$$(3596 \cdot 5597 \cdot 4582)^2 \equiv (2^{10} \cdot 3 \cdot 5 \cdot 11 \cdot 43)^2 \mod 8909.$$

Potenziali fattori di n sono $a + b$ ed $a - b$, con

$$a = 3596 \cdot 5597 \cdot 4582 \mod \text{n}, \qquad \text{b} = 2^{10} \cdot 3 \cdot 5 \cdot 11 \cdot 43 \mod \text{n}.$$

Nel nostro caso, $a = 2352$, $b = 4315$ e

$$\gcd(a + b, n) = 59, \qquad \gcd(a - b, n) = 151.$$