Teoria Elementare dei Numeri 2019 Appello 1 28 gennaio 2020, 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. *Dimostrare che* $\sum_{\bar{x}\in\mathbf{Z}_n} \bar{x} = \bar{0}$ *in* $\mathbf{Z}_n$*, per ogni* n *dispari.*

Sol.: Vedi Esercizi svolti 2008: Foglio 4, n.19.

2. *Sia* N *un intero di 100 cifre e sia* $A = 10^{10}$.
   (a) *Quanti numeri primi ci sono approssimativamente nell'intervallo* $[N - A, N + A]$*?*
   (b) *Quanti numeri* B*-smooth ci sono approssimativamente nell'intervallo* $[N - A, N + A]$*, se* $B = 10^{20}$*?,* $B = 10^{10}$*?* $B = 10^5$*?*

Sol.: (a) La probabilità che un numero casuale di 100 cifre sia primo è stimabile con $\frac{1}{100 \ln n}$, per cui nell'intervallo $[N - A, N + A]$ ci sono approssimativamente $2 * 10^{10} * \frac{1}{100 \ln n} \sim 86858896$ primi.

(b) La probabilità che un numero casuale di 100 cifre sia B-smooth è stimabile con $u^{-}u$, dove $u = \log 10^{100}/\log B$ e nell'intervallo $[N - A, N + A]$ ci sono approssimativamente $2 * 10^{10} * u^{-u}$ interi B-smooth.

In particolare, per $B = 10^{20}$, vale $u = log(10^{100}/10^{20}) = 5$ e $2 * 10^{10} * u^{-u} \sim 6400000$.

Per $B = 10^{10}$, vale $u = log(10^{100}/10^{10}) = 10$ e $2 * 10^{10} * u^{-u} \sim 2$

Per $B = 10^5$, vale $u = log(10^{100}/10^5) = 20$ e $2 * 10^{10} * u^{-u} \sim 1/(524288 * 10^{10})$.

3. *Sia* E *la curva di equazione* $Y^2 = X^3 + 1$ *su* $\mathbf{Z}_5$.
   (a) *Verificare che si tratta di una curva ellittica.*
   (b) *Determinare tutti i punti di* $E(\mathbf{Z}_5)$.
   (c) *Esibire un punto di ordine massimo.*

Sol.: (a) Il discriminante della curva è $\Delta = 27 \equiv 2 \not\equiv 0 \mod 5$. Dunque E definisce una curva ellittica su $\mathbf{Z}_5$.

(b) I quadrati in $\mathbf{Z}_5$ sono $Q_7 = \{0, 1, 4\}$, con radici quadrate date rispettivamente da

$$\sqrt{0} = 0, \quad \sqrt{1} = 1, 4, \quad \sqrt{4} = 2, 3.$$

I punti della curva sono sei

$$(0, 1),\ (0, 4) \quad (2, 2),\ (2, 3), \quad (4, 0), \quad \infty.$$

Poiché c'è un solo punto di ordine due (quello con ordinata nulla), il gruppo $E(\mathbf{Z}_5)$ è ciclico di ordine 6.

(c) I punti della curva $\neq \infty$ possono avere ordine 2, 3 e 6. Se prendiamo un punto P con ordinata non nulla, questo ha ordine 6 se e solo se $2P \neq -P$. Se $P = (0, 1)$, abbiamo $2P = (0, 4) = -P$, quindi P ha ordine 3. Se $Q = (2, 2)$, abbiamo $2Q = (0, 4) \neq -Q$, quindi l'ordine di Q è maggiore di 3 e necessariamente uguale a 6.

4. *Rossi e Bianchi sono due utenti che vogliono condividere una chiave segreta mediante il Diffie-Hellman-Merkle key exchange. Si accordano sul primo* $p = 23$ *e la radice primitiva* $g = \bar{5}$*. Una spia intercetta le stringhe* $\overline{21}$ *e* $\overline{14}$ *che i due utenti si scambiano. Qual è la chiave segreta di Rossi e Bianchi?*

Sol: Siano m_R ed m_B le chiavi segrete di Rossi e di Bianchi. Se poniamo ad esempio $m_B = \log_5(14)$, allora $m_R = \log_5(21)$ la chiave segreta si trova come

$$5^{m_R m_B} = 14^{m_R} = 14^{\log_5(21)} \quad \text{oppure} \quad 5^{m_R m_B} = 21^{m_B} = 21^{\log_5(14)} \mod 23.$$

Calcoliamo $m_R = \log_5(21) = \log_5(3) + \log_5(7)$ mediante il calcolo dell'indice. Dalle relazioni

$$-2 \equiv 21 \equiv 3 \cdot 7, \quad 1 \equiv 24 \equiv 2^3 \cdot 3, \quad 2 \equiv 25 \equiv 5^2, \quad -3 \equiv 20 \equiv 2^2 \cdot 5 \qquad \mod 23,$$

tenendo conto che $\log_5(1) = 0$, $\log_5(5) = 1$, $\log_5(-1) = 11$, troviamo le relazioni fra i logaritmi in base 5

$$11 + \log 2 = \log 3 + \log 7, \quad 0 = 3\log 2 + \log 3, \quad \log 2 = 2, \quad 11 + \log 3 = 2\log 2 + 1 \qquad \mod 22.$$

Risolvendo si trova

$$\log(2) = 2, \quad \log(3) = 16, \quad \log 7 = 19,$$

da cui si ottiene $m_R = 13$ e la chiave segreta $K = 14^{13} \equiv 11 \mod 23$.

5. *Sia $n = 38473$ e siano date le seguenti relazioni modulo n*

$$23157^2 \equiv 3 \cdot 5^2 \cdot 7 \cdot 19, \quad 16721^2 \equiv 2 \cdot 3^2 \cdot 5^2 \cdot 19, \quad 22478^2 \equiv 2^3 \cdot 3^5 \cdot 17,$$

$$1392^2 \equiv 2 \cdot 7^2 \cdot 11 \cdot 13, \quad 19021^2 \equiv 2 \cdot 3 \cdot 17 \cdot 19^2, \quad 8741^2 \equiv 2^4 \cdot 7 \cdot 17 \cdot 19.$$

Quali interi sono potenziali fattori non banali di n? (impostare il calcolo).

Sol.: Se ad esempio moltiplichiamo fra loro la terza e la quinta relazione modulo n, otteniamo

$$22478^2 \cdot 19021^2 \equiv 2^3 \cdot 3^5 \cdot 17 \cdot 2 \cdot 3 \cdot 17 \cdot 19^2 \quad \Leftrightarrow \quad (22478 \cdot 19021)^2 \equiv 2^4 \cdot 3^6 \cdot 17^2 \cdot 19^2 \equiv (2^2 \cdot 3^3 \cdot 17 \cdot 19)^2.$$

Se poniamo $a \equiv 22478 \cdot 19021 \mod n$ e $b = 2^2 \cdot 3^3 \cdot 17 \cdot 19 \mod n$, allora

$$\gcd(a + b, n), \qquad \gcd(a - b, n)$$

sono potenziali fattori non banali di n.