TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 8

Esercizio 8.1. Enunciate e dimostrate la caratterizzazione delle terne pitagoriche, come vista a lezione. Dovete quindi mostrare come ridursi a classificare le terne pitagoriche primitive (a, b, c), e poi far vedere che queste sono della forma

$$\begin{cases} a = s^2 - t^2, \\ b = 2st, \\ c = s^2 + t^2, \end{cases}$$

con $s > t$, s e t coprimi, e di diversa parità.

Esercizio 8.2 (Facoltativo). Siano p, q primi dispari distinti, e $n = pq$. Quanti sono i quadrati in $\mathbf{Z}/n\mathbf{Z}$? Quanti di questi sono invertibili, e quanti invece divisori dello zero?

Esercizio 8.3. Alice e Bob giocano a testa o croce per telefono.

Alice pensa i due numeri primi $p = 103$ e $q = 127$ (verificare che siano entrambi congrui a 3 modulo 4), calcola $N = p \cdot q$, e trasmette N a Bob.

Bob le comunica $b = 14$. Alice, che qui è generosa, gli consiglia di ripensarci. (Perché?)

Bob si scusa, e le comunica $b = 5167$. Perché stavolta Alice è soddisfatta?

Si mostri come fa Alice a trovare le quattro radici quadrate di b modulo N, e si spieghi come prosegue il gioco.

Esercizio 8.4. Alice e Bob giocano a testa o croce per telefono.

Alice pensa due numeri primi p, q, calcola $N = p \cdot q$, e trasmette $N = 19781$ a Bob. (Non sarebbe difficile per Bob fattorizzare N, ma supponiamo che N sia troppo grande per questo.)

Bob prende il numero $a = 201$, e calcola $b = a^2 \pmod N$ (fatelo).

Ora Alice gli comunica un'altra radice quadrata di b modulo N, cioè $c = 18925$. Bob ha vinto! Si mostri come fa a dimostrarlo ad Alice, che non si fida troppo.

Esercizio 8.5. Alice e Bob giocano a testa o croce col secondo metodo descritto a lezione, cioè come segue. (Come al solito, i numeri sono molto piccoli, per semplicità.)

Alice comunica a Bob il numero $n = 35319$, dicendogli che è il prodotto di due primi distinti, uno congruo a 1 (mod 4), l'altro congruo a 3 (mod 4). Bob deve indovinare se quello congruo a 1 è il più grande, oppure il più piccolo.

Bob prova a dire "è il più piccolo dei due primi che è congruo a 1 (mod 4)". Alice gli risponde "hai sbagliato", e glie lo dimostra facendo vedere che i primi sono $p = 183 < 193 = q$, e in effetti $n = p \cdot q$, e $p \equiv 3 \pmod 4$, mentre $q \equiv 1 \pmod 4$.

Ma Bob non si fida...

Esercizio 8.6. Riscrivete l'esercizio precedente scambiando i ruoli di Alice e Bob, e trovando voi dei numeri che funzionano. (Guardate gli appunti per i dettagli.)