TRENTO, A.A. 2015/16
CORSO DI ALGEBRA
FOGLIO DI ESERCIZI # 5

Esercizio 5.1. Si calcoli lo sviluppo decimale periodico di

$$\frac{1}{n},$$

per $n = 3, 7, 9, 11, 13, 17, 19$. Se ne discuta il legame con il periodo di $[10]$ in $U(\mathbf{Z}/n\mathbf{Z})$.

Si calcoli anche lo sviluppo decimale periodico di $1/15$. (Per quest'ultimo, si possono vedere gli appunti.)

Esercizio 5.2. Sia $n = pq$, ove p, q sono primi distinti. Siano r, s, t tali che

$$rs + \varphi(n)t = 1.$$

Si mostri che $a^{rs} \equiv a \pmod{n}$ per ogni intero a.
(SUGGERIMENTO: Per $\gcd(a, n) = 1$ questo segue da Eulero-Fermat, come visto a lezione. Si tratta di vedere che la congruenza di cui sopra vale anche se $\gcd(a, n) \neq 1$, e questa parte è facoltativa. In tal caso conviene pensare a cosa può essere, questo massimo comun divisore.)

Esercizio 5.3. Siano p, q primi distinti, e sia $n = pq$. La probabilità che un numero a preso a caso sia relativamente primo con n (ovvero che $(a, n) = 1$) è

$$\frac{\varphi(n)}{n} = \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right).$$

Se $p, q \approx 10^{200}$, si dia una stima della grandezza di $\varphi(n)/n$, ovvero della piccolezza di $1 - \varphi(n)/n$.

Esercizio 5.4. Si scrivano i numeri interi da 0 a 32 in base 2. Come si scrivono i numeri $2^{100} - 1, 2^{100}, 2^{100} + 1$ in base 2?

Esercizio 5.5. Si consideri il seguente schema RSA.

Alice pensa i numeri primi $p = 23$ e $q = 31$, e calcola $n = pq$.

Notate che $26^2 \leq n < 26^3$. Alice calcola $\varphi(n)$, e sceglie $r = 7$.

Prendete un messaggio di otto lettere, il messaggio che Bob vuole inviare a Alice. Dividetelo in quattro gruppi di due lettere. Codificate ogni lettera come un numero fra 0 e 25, secondo lo schema $A \mapsto 0$, $B \mapsto 1$, $\ldots Z \mapsto 25$. Codificate, con il metodo esposto a lezione, ogni coppia di lettere come un numero p_i compreso fra 0 e $26^2 - 1 < n$, per $i = 1, 2, 3, 4$. Ad esempio, se a, b sono le prime due lettere (già espresse come numeri), allora $p_1 = a + b \cdot 26$.

Mostrate come fa Bob a crittare il messaggio, ottenendo $c_i \equiv p_i^r \pmod{n}$.

Mostrate come fa Alice a decifrare il messaggio, calcolando cioè s, e ottenendo $p_i \equiv c_i^s \pmod{n}$.

Esercizio 5.6. Un altro esempio di RSA, visto dalla parte di Alice. Alice sceglie i numeri primi $p = 19$ e $q = 37$, e calcola $n = pq$ e $\varphi(n)$. Notate che n è compreso fra 26^2 e 26^3, dunque si possono crittare coppie di lettere.

Sceglie poi $r = 85$. Verificate che sia $(r, \varphi(n)) = 1$, e calcolate s, t tali che $rs + \varphi(n)t = 1$.

Comunicate r, n a Bob, che dopo un po' vi manda il messaggio

$$550, 87, 182, 35, 87, 446.$$

Decifratelo.

Ah, dopo aver decifrato, come spiegate l'ultima, strana lettera del messaggio di Bob?