Università degli Studi Roma Tre
Corso di laurea in Matematica A.A 2011-2012
Crittografia - Esercitazione n.2
14 Marzo 2012
Antonio Cigliola

Teoria elementare dei numeri

Esercizio 1. Dimostrare che per ogni $n \in \mathbb{N}$, il numero $n^7 - n$ è divisibile per 42.

Esercizio 2. Risolvere i seguenti sistemi di congruenze:

(i) $\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 5 \pmod 4 \\ x \equiv 3 \pmod 5; \end{cases}$

(ii) $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 7 \pmod{10}; \end{cases}$

(iii) $\begin{cases} x \equiv 1 \pmod 6 \\ x \equiv 8 \pmod{15}; \end{cases}$

(iv) $\begin{cases} 3x \equiv 1 \pmod{10} \\ 4x \equiv 2 \pmod 7; \end{cases}$

(v) $\begin{cases} 3x \equiv 2 \pmod 4 \\ 2x \equiv 7 \pmod{15} \\ 4x \equiv -1 \pmod 7; \end{cases}$

(vi) $\begin{cases} 3x \equiv 2 \pmod 4 \\ 2x \equiv 7 \pmod{15} \\ 4x \equiv -1 \pmod 7; \end{cases}$

Esercizio 3. Determinare l'ultima cifra di 7^{2011} e le ultime due cifre di 15^{1861}

Esercizio 4. Dimostrare che per ogni $n \in \mathbb{N}$:

(i) l'ultima cifra di 7^{4n+1} è 7;

(ii) l'ultima cifra di 2^{4n+3} è 8;

(iii) l'ultima cifra di 3^{4n+1} è 3;

(iv) l'ultima cifra di 4^{2n+3} è 4;

(v) l'ultima cifra di 3^{4n+3} è 7;

(vi) l'ultima cifra di 7^{4n+2} è 9;

(vii) l'ultima cifra di 9^{2n+1} è 9;

(viii) l'ultima cifra di 6^{n+1} è 6;

(ix) le ultime due cifre di 5^{n+2} sono 25;

(x) le ultime cifre di 26^{n+1} sono 76.

Esercizio 5. Dimostrare che 67, 97, 193 e 257 sono numeri primi. Calcolare l'ordine moltiplicativo di 2 in $\mathcal{U}(\mathbb{Z}_p)$, al variare di p tra i quattro numeri precedenti.

Esercizio 6. Sia $b \in \mathbb{N}$ e si definisca il polinomio

$$f_b(x) = x^2 - x + b.$$

Si dice che $f_b(x)$ è un *polinomio di Euler* se è un generatore di primi, ovvero se per ogni $x \in \mathbb{N}$, $x < b$ risulta che $f_b(x)$ è un numero primo.

(i) Sia $f_b(x)$ un polinomio di Euler. Provare che per ogni $-b+1 < x < 0$, $f_b(x)$ è un numero primo.

(ii) Provare che se $f_b(x)$ è un polinomio di Euler, allora b è un numero primo.

(iii) Verificare che per $b = 2, 3, 5, 11, 17, 41$ si ottengono polinomi di Euler.

(iv) Provare che per $b \leqslant 50$ questi sono gli unici polinomi di Euler.

(v) Facoltativamente, magari con l'aiuto di un calcolatore elettronico, provare che quelli sono gli unici polinomi di Euler per $b \leqslant 1000$.

Esercizio 7. Con quanti zeri terminano 20!, 53! e 170!?

Esercizio 8. Provare che per ogni $n \in \mathbb{N}$ i numeri seguenti sono composti:

(i) $2^{10n+1} + 19$;

(ii) $2^{4n+1} + 7$;

(iii) $13^{2n+1} + 17$;

(iv) $2^{2^{10n+1}} + 19$;

(v) $2^{2^{4n+1}} + 7$.

Esercizio 9. Sia dato $a \in \mathbb{N}$. Calcolare le ultime due cifre del numero a^{100} modulo 125.

Esercizio 10. Si determini il resto della divisione per 3 del numero 89741^{527}

Esercizio 11. Si determini il resto della divisione per 9 del numero 57432^{1142}

Esercizio 12. Provare che per ogni $n \in \mathbb{N}$ il numero $2n^{17} + 2n^{15} + 3n^3 + 3n$ è divisibile per 5.

Esercizio 13. Siano dati $n, m \in \mathbb{N}$ due numeri naturali tali che $n \leqslant m$. Descrivere un algoritmo conveniente per il calcolo di

$$n!^n \pmod{m}.$$

Esplicitare la complessità computazionale di tale metodo.

Esercizio 14. Siano $a, b, c, p \in \mathbb{N}$ numeri naturali tali che $a, b, c < p$ e p è un numero primo. Provare che

$$\mathfrak{T}(a^{b^c} \bmod p) \in \mathcal{O}(\log^3 p).$$

Esercizio 15. (3pt) Siano dati due numeri naturali $n \geq 2$ e $d \geq 1$. Si consideri l'anello quoziente $R = \mathbb{Z}_n[x]/(x^d)$.

(a) Calcolare la cardinalità di R.

(b) Provare che l'addizione in R comporta una complessità computazionale di $\mathcal{O}(\log n^d)$.

(c) Provare che la moltiplicazione in R comporta una complessità computazionale di $\mathcal{O}(\log^2 n^d)$.

Crittosistema RSA

Esercizio 16. Sia dato l'alfabeto di 25 caratteri:

,	:	A	B	...	T	U	V	Z	.
0	1	2	3	4	...	20	21	22	23	24

Si supponga di voler spedire il seguente messaggio:

> CONSIDERATE LA VOSTRA SEMENZA:
> FATTI NON FOSTE A VIVER COME BRUTI,
> MA PER SEGUIR VIRTUTE E CANOSCENZA.

ad un utente RSA con chiave pubblica $(N,\ e) = (26899, 25715)$.

(a) Predisporre la spedizione del messaggio coerentemente con i parametri forniti, notando che l'andare a capo equivale ad uno spazio.

(b) Inviare un pacchetto a scelta del messaggio.

Esercizio 17. Nel 2 Agosto del 47 a.C. il generale Caio Giulio Cesare riportò una schiacciante e straordinaria vittoria contro l'esercito di Farnace a Zela nel Ponto. Per stupire il Senato e per sottolineare la rapidità della vittoria, decise di riassumere la situazione con una frase breve e d'effetto. Lo storico Svetonio nel '*De vita Caesarum, Divus Iulius, 37, 1*' racconta:

> *Pontico triumpho inter pompae fercula trium verborum praetulit titulum 'VENI, VIDI, VICI', non acta belli significantem sicut ceteris, sed celeriter confecti notam.*

In massima segretezza, fino alle celebrazioni coram populo del trionfo, vogliamo comunicare al Senato un messaggio da parte del generale, lavorando con un alfabeto di 22 simboli così composto:

A	B	...	V	Z
0	1	2	...	20	21

Le coppie RSA pubbliche di Cesare e del Senato sono rispettivamente (989, 73) e (1363, 3).

Esercizio 18. C'era una volta, in un regno molto lontano, un giovane poeta di nome Valerio, innamorato di una giovane nobildonna, la bellissima Clodia. Quando l'amore era corrisposto e felice, quando la giovane Clodia diceva al suo amato di non voler tenere tra le sue braccia neppure Giove in persona, i due innamorati per poter comunicare in tutta segretezza i loro messaggi d'amore concordarono l'alfabeto latino così composto:

A	B	...	K	L	...	V	X	Y	Z
0	1	2	...	10	11	...	21	22	23	24

e le chiavi pubbliche RSA (1081, 101) per Valerio e (4897, 3011) per Clodia.

Ben presto però Clodia si rivelò una persona meschina e calcolatrice, un'approfittatrice senza scrupoli che viveva in modo libertino rispetto ai restrittivi costumi dell'epoca. Si racconta persino che in tribunale, il grande oratore Marco Tullio abbia accusato la ragazza di adulterio commesso con suo fratello Clodio.

Scoperti i numerosi tradimenti e la vera indole della ragazza, Valerio, sempre più incapace di voler bene a Clodia ma comunque ancora innamorato di lei, decise di mandarle un breve messaggio di addio, esprimendole i suoi sentimenti di rabbia e delusione, ma anche la forza della sua ardente passione.

Le inviò il seguente messaggio cifrato in pacchetti trigrafi:

$$ATV \quad BZG \quad GIF \quad --A \quad DQ-$$

Si dice che di lì a poco il giovane poeta morì, consumato dal dolore e dalla disperazione, lasciandoci tuttavia la più bella raccolta di poesie d'amore che ancora oggi ispira gli innamorati di tutte le età.