NUMERI PRIMI E CRITTOGRAFIA

Parte I. Crittografia a chiave simmetrica

dall'antichità all'era del computer

Parte II. Note della Teoria dei Numeri

concetti ed algoritmi a supporto della Crittografia

Parte III. Crittografia a chiave pubblica

il superamento del problema dello scambio delle chiavi

Parte IV. Esercitazione di gruppo

implementazione di un minisistema crittografico RSA

Tutor: Franco Danielli (franco.danielli@tin.it)

PARTE II

CONCETTI ED ALGORITMI DELLA TEORIA DEI NUMERI

- Lemma di Divisione, Divisibilità
- Numeri Primi: definizione, proprietà
- Generazione di numeri primi
- Massimo Comune Divisore, Algoritmo Euclideo
- Aritmetica modulare e Classi di Congruenza
- Concetto di numero inverso
- Teoremi di Fermat e di Eulero
- Criteri di primalità, Test di Miller-Rabin
- Accorgimenti di calcolo in Aritmetica modulare

Aritmetica dei Numeri Interi

Sia $\mathbb{Z}$ l'insieme dei numeri interi:

$\mathbb{Z}$ = {…… -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ……}

Se *a, b* sono numeri interi, allora i risultati delle operazioni di

Somma (Differenza) = $a \pm b$

Prodotto = $a \cdot b$

Potenza = a^b $(b > 0)$

} sono ancora numeri interi

↓

L'insieme dei numeri interi è **chiuso** per le operazioni di addizione/sottrazione, moltiplicazione, elevazione a potenza.

Introduzione all'Aritmetica modulare: il Lemma di Divisione

siano a (dividendo), d (divisore) due numeri interi, con $d > 0$

Allora, dividendo a per d otterremo altri due numeri interi

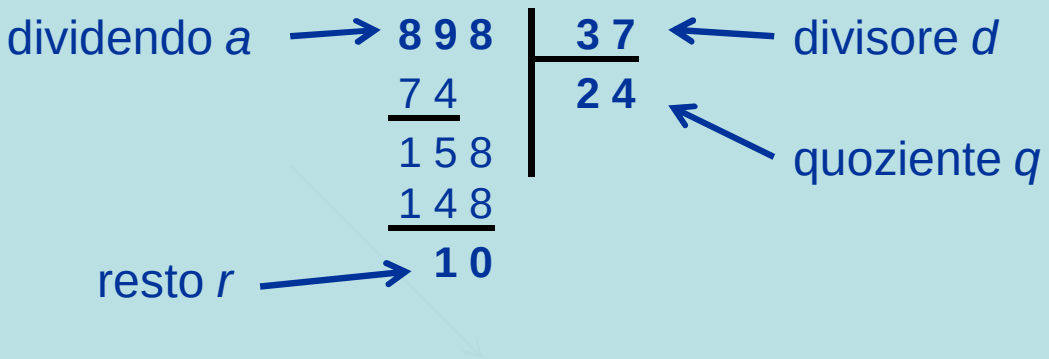
q (quoziente), r (resto), con $0 \leq r < d$, tali che

$$a = d \cdot q + r$$

Esempio:
$a = 898$, $d = 37$

quoziente $q = 24$
resto $r = 10$

Schema di calcolo della divisione:



Relazione di Divisibilità

Siano *a, d* due numeri interi (dividendo, divisore).

Se applicando il Lemma di Divisione risulta

$$r = 0 \quad \Rightarrow \quad \boxed{a = d \cdot q}$$

allora si dice che:

- *a* è divisibile per *d*
- *d* è un divisore di *a*
- *d* divide *a*

} in simboli: $d|a$

Esempio:

$a = 105; \quad d = 21;$

Poiché $105 = 21 \times 5 + 0 \Rightarrow d \mid a$

Proprietà della relazione di divisibilità

n°	Se:	Allora:
1	$d \mid a$	$d \mid -a$; $-d \mid a$; $-d \mid -a$
2	$d \mid a$; $a \mid b$	$d \mid b$
3	$d \mid a$; $a \neq 0$	$1 \leq \lvert d \rvert \leq \lvert a \rvert$
4	a qualunque	$1 \mid a$; $a \mid a$
5	$d \mid a$; $a \mid d$	$\lvert a \rvert = \lvert d \rvert$ $(a = \pm d)$
6	$d \mid 1$	$d = \pm 1$
7	d qualunque	$d \mid 0$
8	$d \mid a$; $d \mid b$	$d \mid m \cdot a + n \cdot b$
9	$d \mid a$; $d \mid (a+b)$	$d \mid b$

Criteri di divisibilità

Un numero *n* (rappresentazione in base decimale) è divisibile per:

d =	Condizione da verificare	Esempio
2	se *n* è pari (ultima cifra = 0, 2, 4, 6, 8)	2 | 123.122
3	se 3 divide la somma delle cifre di *n*	3 | 123.123
4	se 4 divide il numero formato dalle ultime 2 cifre di *n*	4 | 123.124
5	se l'ultima cifra di *n* è 0 oppure 5	5 | 123.125
6	se *n* è pari e divisibile per 3	6 | 123.126
8	se 8 divide il numero formato dalle ultime 3 cifre di *n*	8 | 123.128
9	se 9 divide la somma delle cifre di *n*	9 | 123.129
10	se l'ultima cifra di *n* è 0	10 | 123.130
11	se 11 divide la somma a segni alterni delle cifre di *n*	11 | 123.134

Numeri Primi

Definizione: un numero intero p si dice primo se

- $p \geq 2$
- p ha solo 2 divisori positivi: 1, p

In alternativa: un numero intero $a \geq 2$ non è primo (è composto) se esistono due interi $b, c > 1$ tali che $a = b \cdot c$

Tabella dei 25 numeri primi $p \leq 100$:

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97					

Proprietà dei Numeri Primi

- Unicità della scomposizione in fattori primi

  (Teorema fondamentale dell'Aritmetica):

  Ogni numero intero $a \geq 2$ si può scrivere in modo unico come prodotto di numeri primi (eventualmente con ripetizioni):

  $a = p_1 \cdot p_2 \cdot \ldots \cdot p_n$

  Esempio: $a = 1.165.626 = 2 \times 3 \times 3 \times 7 \times 11 \times 29 \times 29$

- Esistono infiniti numeri primi (Euclide)

- Principio di Euclide:

  Se un primo p divide il prodotto $a \cdot b$, allora p divide almeno uno dei fattori: $p|a \cdot b \Rightarrow p|a$ oppure $p|b$

- Struttura dei numeri primi $p > 3$: $p = 6 \cdot k \pm 1$

Metodi di ricerca di numeri primi

- Metodo del Crivello di Eratostene, Metodo di Divisione:

  ricerca dei numeri primi $p \leq N$, con N dato

- Metodo di Moltiplicazione:

  ricerca dei numeri primi p in un intervallo dato: $N_1 \leq p \leq N_2$

- Test di Primalità:

  Applicazione iterativa di un test efficiente di primalità (esempio: Test di Miller-Rabin) partendo da un numero dispari N, ed incrementandolo a passi di 2 fino al successo (strategia *cut and try*)

Esempio di ricerca di un numero primo col Test di Primalità

- Si vuole trovare un numero primo di 6 cifre, nell'intorno di 900.000 circa.
- Si inizia da un numero casuale dispari, cifra finale 1, 3, 7, 9: sia p = 902.251 il candidato iniziale alla primalità.
- Se p supera il test, p è il primo cercato; se no, lo si aumenta a passi di 2 (saltando la cifra finale 5), e si ripete il test fino al successo:

Trial	p	*Test:* p è primo?
1	902.251	Falso
2	902.253	Falso
3	902.257	Falso
4	902.259	Falso
5	902.261	Vero

p = 902.261
è un numero primo
che soddisfa i criteri
di ricerca

Questioni aperte sui numeri primi

- Congettura di Goldbach: qualunque numero pari $n \geq 4$ si può scrivere come somma di 2 numeri primi. La congettura è stata verificata fino a numeri n grandissimi, ma mai dimostrata.

  Esempi:
  $4 = 2 + 2$
  $6 = 3 + 3$
  $8 = 5 + 3$
  $12 = 7 + 5$
  $20 = 13 + 7 = 17 + 3$
  $100 = 59 + 41 = 71 + 29$
  $1000 = 983 + 17 = 509 + 491$

- Le coppie di numeri primi "gemelli" (p, q tali che $p - q = 2$) sono infinite? I matematici ritengono di si, ma anche questa congettura non è mai stata dimostrata.

  Esempi di primi gemelli: 11, 13 17, 19 29, 31 41, 43 ecc.

Massimo Comune Divisore (MCD)

- Dati due numeri interi *a, b* (con $b \neq 0$), si dice Massimo Comune Divisore il più grande numero intero positivo d che li divide entrambi:

$$d = \text{MCD}(a, b)$$

- Il MCD è anche la più piccola combinazione lineare positiva che si possa costruire su *a, b* con coefficienti interi *s, t*:

$$d = \text{MCD}(a, b) = s \cdot a + t \cdot b$$

- Se MCD (*a, b*) = 1 allora *a, b* si dicono relativamente primi

Esempio: determinare il MCD (40, 24)

divisori di 40: 1, 2, 4, 5, 8, 10, 20, 40

divisori di 24: 1, 2, 3, 4, 6, 8, 12, 24

divisori comuni: 1, 2, 4, 8 $\Rightarrow$ MCD(40, 24) = 8

Proprietà del Massimo Comune Divisore

n°	Se:	Allora:
1	a qualunque , $b = 0$	$MCD\ (a, 0) = \lvert a \rvert$
2	d = MCD (a, b); $m \mid d$	$m \mid a$; $m \mid b$
3	d = MCD(a, b)	$\exists!\ s, t : s \cdot a + t \cdot b = d$
4	$a \mid b \cdot c$; MCD$(a, b) = 1$	$a \mid c$
5	p primo; p non divide a	MCD$(a, p) = 1$
6	$m \mid a$; $n \mid a$; MCD$(m, n) = 1$	$m \cdot n \mid a$

Esempio: $a = 10$; $p = 7$ $\Rightarrow$ p primo, p non divide a

$\Rightarrow$ MCD(10, 7) = 1 (proprietà n° 4)

Scegliendo i numeri interi: $s = 5$; $t = -7$

$\Rightarrow$ 5 x 10 – 7 x 7 = 1 (proprietà n° 2)

Algoritmo Euclideo

È il più efficiente metodo di calcolo del MCD di due numeri interi *a, b* assegnati, non entrambi nulli (Euclide, III aC).

La brillante idea risolutiva è costituita dall'applicazione ricorsiva del Lemma di Divisione, e sfrutta una delle proprietà già viste della relazione di Divisibilità:

1. $a = b \cdot q_1 + r_1 \quad \Rightarrow \; r_1 = a - b \cdot q_1 \quad \Rightarrow \; \text{MCD}(a,b) = \text{MCD}(b,r_1)$
2. $b = r_1 \cdot q_2 + r_2 \quad \Rightarrow \; r_2 = b - r_1 \cdot q_2 \quad \Rightarrow \; = \text{MCD}(r_1,r_2)$
3. $r_1 = r_2 \cdot q_3 + r_3 \quad \Rightarrow \; r_3 = r_1 - r_2 \cdot q_3 \quad \Rightarrow \; = \text{MCD}(r_2,r_3)$
4. … … … … … … … … … … …

- $r_{n-2} = r_{n-1} \cdot q_n + r_n \quad \Rightarrow \; r_n = r_{n-2} - r_{n-1} \cdot q_n \quad \Rightarrow \; = \text{MCD}(r_{n-1},r_n)$
- $r_{n-1} = r_n \cdot q_{n+1} + 0 \quad \Rightarrow r_{n+1} = 0$: STOP $\Rightarrow \; = \text{MCD}(r_n,0) = r_n$

Il risultato è l'ultimo resto non nullo del procedimento:

$d = \text{MCD}(a, b) = r_n$

Esempio di applicazione dell'Algoritmo Euclideo

Si vuole calcolare d = MCD(a, b), con a = 1.634, b = 627:

Step	Dividendo	Divisore	Quoziente	Resto
1	1.634	627	2	380
2	627	380	1	247
3	380	247	1	133
4	247	133	1	114
5	133	114	1	19
6	114	19	6	0

L'ultimo resto non nullo (step 5) è il risultato cercato:

d = MCD (1.634, 627) = 19

Aritmetica Modulare: l'operatore mod

a è un numero intero qualunque, n un modulo > 0

Esprimiamo il resto r applicando il Lemma di Divisione:

$$r = a - n \cdot q$$

La stessa relazione si esprime in modo equivalente:

$$r = a \bmod n$$

("r uguale ad a modulo n")

Osservazione:

- $a \in \mathbb{Z}$ può assumere infiniti valori,
- r ne può assumere soltanto n: $r \in \{0, 1, 2, 3, \dots , n-1\}$
- $\Rightarrow$ l'Aritmetica Modulare è un'aritmetica finita

Aritmetica Modulare: Esempi

47 mod 10 = 7
47 mod 9 = 2
47 mod 8 = 7
47 mod 7 = 5
47 mod 6 = 5
47 mod 5 = 2
47 mod 4 = 3
47 mod 3 = 2
47 mod 2 = 1

27 mod 10 = 7
27 mod 9 = 0
27 mod 8 = 3
27 mod 7 = 6
27 mod 6 = 3
27 mod 5 = 2
27 mod 4 = 3
27 mod 3 = 0
27 mod 2 = 1

Esercizi:
(14 x 12) mod 10 = ?
(14 x 12) mod 13 = ?
(4 x 9) mod 12 = ?

Congruenza modulo *n*

- Siano *a*, *b* numeri interi, ed $n > 0$ un modulo
- Se il modulo *n* divide la differenza (*a* – *b*), allora si dice che "*a* è congruo a *b* modulo *n*" e vale la notazione:

$$n|(a - b) \quad \Leftrightarrow \quad a \equiv b \pmod{n}$$

- Equivalentemente: $a \equiv b \pmod{n} \quad \Leftrightarrow \quad a \bmod n = b \bmod n$

Esempi:

a	*b*	*n*	$a \equiv b \pmod{n}$?
1237	87	10	$1237 \equiv 87 \pmod{10}$
-25	1	13	$-25 \equiv 1 \pmod{13}$
9	5	2	$9 \equiv 5 \pmod{2}$
9	4	2	$9 \not\equiv 4 \pmod{2}$

Proprietà delle congruenze modulo *n*

n°	Se:	Allora:
1	$a \equiv b \pmod{n}$, k qualunque	$a + k \equiv b + k \pmod{n}$ $a \cdot k \equiv b \cdot k \pmod{n}$
2	$k \cdot a \equiv k \cdot b \pmod{n}$; $\mathrm{MCD}(k, n) = 1$	$a \equiv b \pmod{n}$
3	$a \equiv b \pmod{n}$; $c \equiv d \pmod{n}$	$a + c \equiv b + d \pmod{n}$ $a \cdot c \equiv b \cdot d \pmod{n}$
4	$a \equiv b \pmod{n}$; $k > 0$	$a^k \equiv b^k \pmod{n}$

Classi di congruenza modulo *n*

Fissato un modulo intero $n > 0$, consideriamo la partizione dell'insieme dei numeri interi in n sottoinsiemi secondo lo schema seguente ($n = 7$):

$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
..	..	..	..	..	..	..
-28	-27	-26	-25	-24	-23	-22
-21	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34
..	..	..	..	..	..	..

Tali sottoinsiemi prendono il nome di Classi di congruenza (ovvero Classi di resto) modulo *n*.

Sulle classi di congruenza si può costruire una Aritmetica con le operazioni di addizione e moltiplicazione.

Proprietà delle classi di congruenza modulo *n*:

- se *a, b* appartengono alla stessa classe $\Rightarrow$ $a \equiv b \pmod{n}$
- se *a, b* appartengono a classi diverse $\Rightarrow$ $a \not\equiv b \pmod{n}$

Notazioni ed esempi di Aritmetica Modulare

Le notazioni seguenti sono fra loro equivalenti, e derivano dal Lemma di Divisione:

$a = n \cdot q + r$

$0 \le r < n$

- $a \bmod n = r$ — operatore mod
- $a \equiv r \pmod{n}$ — relazione di congruenza modulo n
- $a \in [\, r \,]_n$ — classe di resto modulo n

Somma e prodotto in Aritmetica Modulare: notazioni equivalenti

$a = n \cdot q + r$	$a \bmod n = r$	$a \equiv r \pmod{n}$	$a \in [\, r \,]_n$
3x9 = 10x2 + 7	(3x9) mod10 = 7	3x9 ≡ 7 (mod10)	$[3]_{10} \times [9]_{10} = [7]_{10}$
7+5 = 10x1 + 2	(7+5) mod10 = 2	7+5 ≡ 2 (mod10)	$[7]_{10} + [5]_{10} = [2]_{10}$

Concetto di numero inverso

Dato un numero *a*, si dice inverso di *a* quel numero *x* (se esiste) tale che:

$$a \cdot x = 1$$

Nell'Aritmetica dei numeri interi, soltanto i numeri 1 e -1 sono invertibili, e sono precisamente gli inversi di se stessi:

$1 \times 1 = 1$ $\quad$ $-1 \times (-1) = 1$

Nell'Aritmetica modulare invece esistono in generale elementi diversi da ±1 che si possono invertire:

$$a \cdot x \equiv 1 \pmod{n}$$

Ad esempio, modulo 10, ci sono 4 elementi invertibili (1, 3, 7, 9), cioè altri 2 oltre a quelli canonici 1, -1 ≡ 9

$$\left.\begin{array}{l} 1 \times 1 = 1 \\ 3 \times 7 = 21 \\ 7 \times 3 = 21 \\ 9 \times 9 = 81 \end{array}\right\} \equiv 1 \pmod{10}$$

Invertibilità in Aritmetica modulare

Modulo n, sono invertibili solo quelle classi di resto $[a]_n$ con a relativamente primo rispetto ad n, cioè tali che:

$$\text{MCD}(a, n) = 1$$

Esempio: $n = 9$

a	$d = \text{MCD}(a, n)$	$a^{-1} \bmod n$	$a \cdot a^{-1} \bmod n$
0	9	-	
1	1	1	$1 \equiv 1 \pmod 9$
2	*1*	*5*	$10 \equiv 1 \pmod 9$
3	3	-	
4	1	7	$28 \equiv 1 \pmod 9$
5	1	2	$10 \equiv 1 \pmod 9$
6	3	-	
7	1	4	$28 \equiv 1 \pmod 9$
8	1	8	$64 \equiv 1 \pmod 9$

Modulo 9

le classi di resto invertibili sono 6:

1, 2, 4, 5, 7, 8

La funzione di Eulero $\Phi(n)$

Dato un numero intero $n > 0$ (modulo), questa funzione conta il numero di classi di resto invertibili mod n, ovvero quanti sono gli elementi $0 \le a < n$ *tali che* MCD(a, n) = 1, cioè relativamente primi rispetto ad n.

$\Phi(n)$ si calcola dalla fattorizzazione di n, secondo l'espressione seguente:

$$n = p_1^{\alpha} \cdot p_2^{\beta} \cdot \ldots \quad \Rightarrow \quad \Phi(n) = (p_1 - 1) \cdot p_1^{(\alpha - 1)} \cdot (p_2 - 1) \cdot p_2^{(\beta - 1)} \cdot \ldots$$

Esempio: $n = 36 = 2^2 \times 3^2 \quad \Rightarrow \quad \Phi(n) = 1 \times 2 \times 2 \times 3 = 12$

Valori di $\Phi(n)$ per $n = 1 \div 20$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\Phi(n)$	0	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8	16	6	18	8

Osservazione
Se p è un numero primo, allora $\Phi(p) = p - 1$:
eccettuata la classe 0, tutte le classi di resto mod p sono invertibili.

Tabella di invertibilità modulo n:

modulo n = 10 (composto)

0	1	2	3	4	5	6	7	8	9
1	•								
2									
3							•		
4									
5									
6									
7			•						
8									
9									•

$\Phi(10) = 4$
ci sono 4 elementi
invertibili: 1, 3, 7, 9

modulo n = 11 (primo)

0	1	2	3	4	5	6	7	8	9	10
1	•									
2						•				
3				•						
4			•							
5									•	
6		•								
7								•		
8							•			
9					•					
10										•

$\Phi(11) = 10$
tutti gli elementi $\neq 0$
sono invertibili

Calcolo dell'inverso modulo *n*

Se *a* è un numero intero, relativamente primo rispetto ad un modulo $n > 0$, allora esistono coppie di numeri interi *s, t* tali che:

$$\text{MCD}(a, n) = 1 = s \cdot a + t \cdot n$$

Poiché: $(s \cdot a + t \cdot n) \bmod n = (s \cdot a) \bmod n$, vale che:

$$s \cdot a \equiv 1 \pmod{n}$$

e quindi, modulo *n*, *s* è precisamente l'inverso cercato di *a*.

L'inverso di *a* mod *n* si calcola applicando l'algoritmo euclideo in forma estesa (coefficiente *s* di Bezout).

L'algoritmo è stato implementato nel foglio di calcolo Excel "**Inverso_Mod_n.xls**".

(Piccolo) Teorema di Fermat

Se p è un numero primo, ed a un intero qualunque, allora vale che:

$$a^{p} \equiv a \pmod{p}$$

Se a e p sono relativamente primi, si può semplificare per a:

$$\text{MCD}(a, p) = 1 \quad \Rightarrow \quad a^{p-1} \equiv 1 \pmod{p}$$

Esempio: p = 7

a	$a^6 = n \cdot q + r$	a^6 mod 7
1	$1^6 = 1 = 7 \times 0 + 1$	1
2	$2^6 = 64 = 7 \times 9 + 1$	1
3	$3^6 = 729 = 7 \times 104 + 1$	1
4	$4^6 = 4.096 = 7 \times 585 + 1$	1
5	$5^6 = 15.625 = 7 \times 2.232 + 1$	1
6	$6^6 = 46.656 = 7 \times 6.665 + 1$	1

Generalizzazione del Teorema di Fermat: il Teorema di Eulero

Se $n > 0$ è un modulo (non necessariamente primo), $\Phi(n)$ la sua funzione di Eulero, ed a un intero qualunque relativamente primo rispetto ad n, allora vale che:

$$a^{1+\Phi(n)} \equiv a \pmod{n}$$

Poiché a ed n sono relativamente primi, si può semplificare per a:

$$\text{MCD}(a, n) = 1 \quad \Rightarrow \quad a^{\Phi(n)} \equiv 1 \pmod{n}$$

Esempio: $n = 12$; $\Phi(n) = 4$

a	$a^4 = n \cdot q + r$	a^4 mod 12
1	$1^4 = 1 = 12 \times 0 + 1$	1
5	$5^4 = 625 = 12 \times 52 + 1$	1
7	$7^4 = 2.401 = 12 \times 200 + 1$	1
11	$11^4 = 14.641 = 12 \times 1.220 + 1$	1

Criterio probabilistico di primalità: l'Algoritmo di Miller - Rabin

Si basa sull'applicazione del Teorema di Fermat:

Sia: N il numero (dispari) candidato alla primalità

1. Si genera un numero casuale a nel range $2 \leq a \leq N - 2$
2. Si calcola $d = \text{MCD}(a,N)$: se $d > 1$, N non è primo: test fallito, si cerca un altro N
3. Se $d = 1$, scriviamo N nella forma $N = 2^s \cdot t + 1$, $s \geq 1$, t dispari
   - Se $a^t \bmod N = 1 \Rightarrow N$ supera il test: OK
   - Se no, detto $e = 2^r \cdot t$ per $r = 0, 1, 2, \ldots, s - 1$, se $a^e \equiv -1 \pmod N$ per almeno un valore di $r \Rightarrow N$ supera il test: OK
4. Se N supera il punto 3, si riparte dal punto 1 e si riesegue il test per complessive k volte: se il risultato è sempre OK, N è primo a meno di una probabilità su 4^k (se $k = 20$, 1 probabilità su 10^{12})
5. Se N fallisce anche un solo ciclo, N non è primo, si cerca un altro N

Accorgimenti di calcolo in Aritmetica Modulare (1)

Si voglia eseguire il calcolo: $x = 7^{12} \bmod 13$

Una prima idea può essere quella di condurre il calcolo in Aritmetica ordinaria, e di ridurre modulo *n* il risultato finale.

Nel nostro caso:
$7^{12} = 13.841.287.201$

Applicando il Lemma di Divisione:
$13.841.287.201 = 13 \times 1.064.714.400 + 1 \equiv 1 \pmod{13}$

Risultato: $x = 1$

Nota: il metodo è scarsamente efficiente, diventa presto impraticabile per la complessità dei calcoli da eseguire!

Accorgimenti di calcolo in Aritmetica Modulare (2)

Una strategia molto più efficiente è quella di condurre opportunamente il calcolo a passi, riducendo modulo *n* ogni risultato intermedio.

Nell'esempio precedente: $x = 7^{12} \bmod 13$

1° passo: $a = 7^2 = 49 \equiv -3 \pmod{13}$
2° passo: $b = 7^4 = a^2 \equiv 9 \pmod{13} \equiv -4 \pmod{13}$
3° passo: $c = 7^8 = b^2 \equiv 16 \pmod{13} \equiv 3 \pmod{13}$
4° passo: $d = b \cdot c = 7^4 \times 7^8 = 7^{12} \equiv -12 \pmod{13} \equiv 1 \pmod{13}$

Lo stesso risultato finale: $x = 7^{12} \bmod 13 = d \bmod 13 = 1$

è stato ottenuto molto più agevolmente, senza nemmeno dover usare un calcolatore.

Nota: si poteva prevedere subito il risultato senza fare alcun calcolo?