1. Aritmetica Modulare e Applicazioni

Le parti precedute dal simbolo ▶ (adattate dal sistema di aiuto in linea del programma Scientific Workplace) si riferiscono alle procedure da seguire per svolgere i conti col computer e fanno parte solo della versione "interattiva" della lezione. Non sono necessarie per la preparazione allo scritto.

1.1. Equazioni diofantine

Le *equazioni Diofantine* più semplici sono equazioni della forma $ax + by = c$ dove a, b e c sono *numeri interi*. Si cercano soluzioni in cui x e y sono anch'essi *numeri interi*. Una condizione necessaria e sufficiente per la sua risolubilità in numeri interi è che c sia divisibile per il *Massimo Comun Divisore* (gcd) *di* a e b . La necessità della condizione è ovvia, un esempio chiarisce il metodo di risoluzione (e, con esso, la sufficienza).

Esempio: $122x+184y = 42$ è risolubile perchè 42 è divisibile per $\gcd(122, 184) = 2$. Dividendo si ottiene $61x + 92y = 21$. Si osservi che, se si conosce una soluzione particolare di $61x + 92y = 1$, allora moltiplicando la soluzione per 21 si trova una soluzione particolare dell'equazione originale. Per trovare una soluzione particolare basta impostare *l'algoritmo euclideo* delle divisioni successive fino a ottenere come resto finale il $\gcd(61, 92) = 1$.

$\frac{92}{61} = 1 + \frac{31}{61}$, $\frac{61}{31} = 1 + \frac{30}{31}$, $\frac{31}{30} = 1 + \frac{1}{30}$

Allora si ottiene, partendo dalla prima, e scrivendo via via tutti i resti in funzione dei numeri di partenza:

$31 = 92 - 61$, $30 = 61 - 92 + 61$, $1 = 92 - 61 - 61 - 61 + 92$

Cioè:

$61 \times (-3) + 92 \times 2 = 1$

Allora una soluzione particolare dell'equazione è $x = 21 \times (-3) = -63$ e $y = 21 \times 2 = 42$. Ovviamente la soluzione generale si trova sommando alla soluzione particolare tutte le (infinite) *soluzioni intere* di $61x + 92y = 0$ ($x = -92k$, $y = 61k$ con k intero arbitrario). In definitiva si ottiene che tutte le soluzioni intere di: $122x + 184y = 42$ sono date da:

$x = -63 - 92k$ e $y = 42 + 61k$.

▶ Solve + Integer

$$122x + 184y = 42, \text{ Solution is : } \{x = -63 - 92N_1, y = 42 + 61N_1\},$$

L'intero k usato prima è rimpiazzato, dal programma, da N_1.

▶ Solve + Integer

$$\begin{matrix} 3x+2y=5 \\ 3x-z=1 \end{matrix}, \text{Solution is}: \{x=5-2N_1, y=-5+3N_1, z=-6N_1+14\}$$

Infatti: $3x+2y = 3(5-2N_1)+2(-5+3N_1) = 5$ e $3x-z = 3(5-2N_1) - (-6N_1+14) = 1$.

1.2. Congruenze, resti e la funzione "mod(n)".

Due numeri interi a e b sono *congruenti modulo* m quando $a-b$ è un multiplo di m, in questo caso si scrive: $a \equiv b \pmod m$. Ad esempio, $15 \equiv 33 \pmod 9$, infatti $15-33 = -18$ che è multiplo di 9.

Dati due interi a e m, la *funzione modulo* è data da: $a \bmod m = b$ se e solo se $a \equiv b \pmod m$ e $0 \leq b \leq m-1$; quindi, $a \bmod m$ è il più *piccolo resto non negativo* della divisione di a per m.

▶ Per calcolare la funzione mod

1. Selezionare l'espressione $a \bmod b$.
2. Selezionare Evaluate.

▶ Evaluate

$23 \bmod 14 = 9$ mentre invece $(-23) \bmod 14 = 5$

Infatti: $23 = 1\times14+9$, mentre, se vogliamo un resto positivo, $-23 = -2\times14+5$

Se a è positivo, si può trovare il valore di a modulo m anche applicando Expand al quoziente $\frac{a}{m}$.

▶ Expand

$$\frac{23}{14} = 1\frac{9}{14}$$

(in questa notazione, il primo numero è la parte intera del risultato)

Siccome $1\frac{9}{14} = 1+\frac{9}{14}$, la moltiplicazione di $\frac{23}{14} = 1+\frac{9}{14}$ per 14 dimostra che $23 \bmod 14 = 9$.

1.3. Tavole di somma e moltiplicazione Modulo m

Ogni intero a, usando la funzione $\mod m$, si può trasformare in un "numero" appartenente all'insieme $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$ detto *Insieme dei resti positivi delle divisioni per m.* Prendendo la "riduzione modulo m" della somma e della moltiplicazione tra numeri interi usuali si possono definire due nuove operazioni tra *"numeri modulo m"* cioè operazioni tra elementi dell'insieme $\mathbf{Z}_m$. L'importanza di queste operazioni risiede nel fatto che *il risultato di ambedue le operazioni resta all'interno dell'insieme Z_m* : le operazioni si dicono interne.

La somma è definita da:

$$(a \bmod m) + (b \bmod m) = (a + b) \bmod m$$

e il prodotto da:

$$(a \bmod m) \cdot (b \bmod m) = (a \times b) \bmod m.$$

Esempi: $111 \bmod 6 = 3$, $459 \bmod 6 = 3$, $111 \times 459 = 50\,949$ e $111 + 459 = 570$.Si ottiene $50\,949 \bmod 6 = 3$ e $570 \bmod 6 = 0$ cioè $3 \cdot 3 = 3$ e $3 + 3 = 0$

Si noti che, ad esempio, $(2 \times 3) \bmod 6 = 0$ anche se $2 \bmod 6 = 2$ e $3 \bmod 6 = 3$ sono entrambi diversi da 0. Questo è vero in generale: se m non è un numero primo alcuni prodotti (quali?) danno come risultato 0 anche se ambedue i fattori sono, modulo m, diversi da 0.

Per calcolare $-a \bmod m$ ("calcolare" significa in questo caso trovare il resto *positivo* corrispondente) basta osservare che, applicando la definizione di somma si ha:

$$(-a \bmod m) + (a \bmod m) \quad = \quad (a - a) \bmod m = 0$$

e anche:

$$(m - a) \bmod m) + (a \bmod m) = (m + a - a) \bmod m = m \bmod m = 0.$$

Ne consegue che:

$$(-a \bmod m) = (m - a) \bmod m$$

▶ Per ottenere rapidamente la tabella di moltiplicazione modulo m (ad esempio con $m = 6$)

1. Definire la funzione $g(i, j) = (i - 1)(j - 1) \bmod 6$

2. Dal menu Matrices , selezionare Fill Matrix.

3. Selezionare Defined by Function.

4. Scrivere g nel campo Enter Function Name.

5. Selezionare 7 rows e 7 columns.

6. Selezionare OK.

1. Selezionare la matrice e infine Evaluate.

▶ Evaluate

0	0	0	0	0	0
0	1	2	3	4	5
0	2	4	0	2	4
0	3	0	3	0	3
0	4	2	0	4	2
0	5	4	3	2	1

▶ Per migliorare la leggibilità si può procedere così:

1) Fare una copia di questa matrice.

2) Dal menu Edit selezionare Insert Row(s)..., e aggiungere una nuova riga in alto.

3) Selezionare Insert Column(s)..., e aggiungere una nuova colonna a sinistra.

4) Riempire poi gli spazi vuoti come segue:

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dalla tavola vediamo, ad esempio, che $2 \cdot 4 = 2$, $5 \cdot 2 = 4$ e $5 \cdot 5 = 1$ (Le linee orizzontali e verticali e il simbolo della moltiplicazione sono stati aggiunti per maggiore leggibilità)

Se p è primo, ad esempio 7, gli interi modulo p sono particolarmente importanti perchè nella tavola di moltiplicazione lo zero (0) appare solo come risultato di

(0·qualche cosa) e in questa essenziale proprietà ricordano gli usuali numeri interi.

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

1.4. Inversi Modulo m

Se $ab \bmod m = 1$, allora b è detto essere un *inverso* di a *modulo* m, si indica con $a^{-1} \bmod m$ il più piccolo resto positivo della divisione di b per m. L'inverso di a si può trovare semplicemente applicando la definizione: $ab \bmod m = 1$ significa che $ab = 1 + my$, con y intero, cioè si deve risolvere l'equazione diofantina (nelle incognite x e y, ma attenzione, basta trovare la x!):

$$ax - my = 1$$

E poi calcolare $b = x \bmod m$. Spiegheremo dopo (vedi Teorema di Eulero) alcuni metodi più efficienti per trovare (quando esiste!) l'inverso modulo m di un numero.

Se m è un numero primo, ogni $a \neq 0 \bmod m$ possiede un inverso modulo m. Se m non è un numero primo, possiedono inverso modulo m solo i numeri a primi con m. (Nella tavola di moltiplicazione i "numeri modulo m" che possiedono inverso si riconoscono dal fatto che nella loro riga compare il numero uno)

$\gcd(24277, 54) = 1$ allora $24277^{-1} \bmod 54 = 7$

$\gcd(146524, 35) = 7$ allora $146524^{-1} \bmod 35$ non esiste anche se $146524 \bmod 35 = 14 \neq 0$.

▶ Evaluate

$5567^{-1} \bmod 7 = 4$

Infatti $5567 \times 4 \bmod 7 = 1$. Altre notazioni utilizzabili per gli inversi modulo m includono $1/a \bmod m$ e $\frac{1}{a} \bmod m$.

▶Evaluate

$1/23 \bmod 257 = 190$

$\frac{1}{5} \bmod 6 = 5$

La notazione $a/b \bmod m$ va interpretata come $(a \times (b^{-1} \bmod m)) \bmod m$; cioè, trovare l'inverso di b modulo m, moltiplicare il risultato per a, e poi ridurre il prodotto modulo m.

▶ Evaluate

$3/23 \bmod 257 = 56$ (infatti $(3 \times 190) \bmod 257 = 56$)

$\frac{2}{5} \bmod 6 = 4$

1.5. Equazioni Modulo m

Per risolvere una equazione della forma $ax \equiv b \pmod m$ si moltiplicano ambo i membri per $a^{-1} \bmod m$ e si ottiene $x = b/a \bmod m$. Per ottenere $a^{-1} \bmod m$ si veda il paragrafo precedente.

Naturalmente questo si può fare se e solo se $a^{-1} \bmod m$ è diverso da 0.

Esempio: $17x \equiv 23 \pmod{127}$ ha, fra le sue soluzioni, $x = 91$, come illustrato dai seguenti passaggi:

▶ Evaluate

$23/17 \bmod 127 = 91$

▶ Evaluate

$17 \cdot 91 \bmod 127 = 23$

Notare che, siccome 91 è una soluzione di $17x \equiv 23 \pmod{127}$, tutte le altre soluzioni sono date da $91 + 127n$, dove n è un intero qualsiasi. Infatti, $x \equiv 91 \pmod{127}$ vuole dire proprio che $x = 91 + 127n$ per un qualche intero n.

1.6. Coppie di Congruenze lineari

Siccome le congruenze del tipo $ax \equiv b \pmod{m}$ si riducono a $x \equiv c \pmod{m}$, considereremo solo congruenze di questo tipo.

Esempio: siano da risolvere *contemporaneamente* le due congruenze:

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Se i numeri m e n sono *primi fra loro* ($\gcd(m, n) = 1$) ,allora c'è una *unica* soluzione (modulo $m \times n$)

Consideriamo, ad esempio:

$$\begin{aligned} x &\equiv 45 \pmod{237} \\ x &\equiv 19 \pmod{419} \end{aligned}$$

Si trova $\gcd(237, 419) = 1$, così 237 e 419 sono primi fra loro. la prima congruenza fornisce $x = 45 + 237k$ per qualche intero k. Sostituendo nella seconda,

$$45 + 237k = 19 + 419r$$

per un certo r. Questa equazione si può riscrivere $237k = (19 - 45) \bmod 419$, che ha come soluzione:

$$k = (19 - 45)/237 \bmod 419 = 60$$

Quindi,

$$x = 45 + 237 \times 60 = 14265$$

Infatti, $14265 \bmod 237 = 45$ e $14265 \bmod 419 = 19$.

La soluzione generale è data da:

$$x = 14265 + 237 \times 419s$$

Ovvero:

$$x \equiv 14265 \pmod{99303}$$

In generale, *se m e n sono primi fra loro*, le congruenze,

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

danno:

$$x = a + m\,[(b-a)/m \bmod n]$$

La soluzione completa è:

$$x = a + m\,[(b-a)/m \bmod n] + s \times m \times n$$

dove s è un intero arbitrario.

Si osservi che la formula precedente ci dice che, *se m e n sono numeri primi*, se $x \equiv 1 \pmod m$ e $x \equiv 1 \pmod n$ allora $x \equiv 1 \pmod{m \times n}$, infatti $x = 1 + s \times m \times n$. Questa osservazione sarà importante nel seguito.

1.7. Sistemi di Congruenze Lineari

Il cosiddetto *teorema cinese del resto* dice che, *se i moduli sono primi tra loro a coppie*, allora c'è un'unica soluzione modulo il prodotto di tutti i moduli.

$$\begin{aligned} x &\equiv 45 \pmod{237} \\ x &\equiv 19 \pmod{419} \\ x &\equiv 57 \pmod{523} \end{aligned}$$

Si verifica che $\gcd(237 \times 419, 523) = 1$; il sistema ha quindi soluzione. Le prime due congruenze (come visto sopra) sono rimpiazzate da $x \equiv 14265 \pmod{99303}$; quindi il sistema diventa:

$$\begin{aligned} x &\equiv 14265 \pmod{99303} \\ x &\equiv 57 \pmod{523} \end{aligned}$$

Come prima, $14265+99303k = 57+523r$. Così, $k = (57-14265)/99303 \bmod 523 = 134$; quindi $x = 14265 + 99303 \times 134 = 13320867$. Il sistema è quindi risolto da:

$$x \equiv 13320867 \pmod{51935469}$$

1.8. Aritmetica in altissima precisione

I sistemi moderni di computer algebra supportano calcoli con interi di milioni di cifre, come fanno?

Incominciamo a generare un po' di numeri primi fra loro a coppie:

$$(997, 999, 1000, 1001, 1003, 1007, 1009)$$

▶ Factor

$$\begin{bmatrix} 997 \\ 999 \\ 1000 \\ 1001 \\ 1003 \\ 1007 \\ 1009 \end{bmatrix} = \begin{bmatrix} 997 \\ 3^3 37 \\ 2^3 5^3 \\ 7 \times 11 \times 13 \\ 17 \times 59 \\ 19 \times 53 \\ 1009 \end{bmatrix}$$

Consideriamo i numeri 23890864094 e 1883289456. Rappresentiamoli "a pezzi" modulo i numeri trovati prima:

$$23890864094 \longleftrightarrow \begin{bmatrix} 23890864094 \bmod 997 &= 350 \\ 23890864094 \bmod 999 &= 872 \\ 23890864094 \bmod 1000 &= 94 \\ 23890864094 \bmod 1001 &= 97 \\ 23890864094 \bmod 1003 &= 879 \\ 23890864094 \bmod 1007 &= 564 \\ 23890864094 \bmod 1009 &= 218 \end{bmatrix}$$

$$1883289456 \longleftrightarrow \begin{bmatrix} 1883289456 \bmod 997 &= 324 \\ 1883289456 \bmod 999 &= 630 \\ 1883289456 \bmod 1000 &= 456 \\ 1883289456 \bmod 1001 &= 48 \\ 1883289456 \bmod 1003 &= 488 \\ 1883289456 \bmod 1007 &= 70 \\ 1883289456 \bmod 1009 &= 37 \end{bmatrix}$$

Thus, the product $23890864094 \cdot 1883289456$ is represented by the vector

$$\begin{bmatrix} 350 \cdot 324 \bmod 997 &= 739 \\ 872 \cdot 630 \bmod 999 &= 909 \\ 94 \cdot 456 \bmod 1000 &= 864 \\ 97 \cdot 48 \bmod 1001 &= 652 \\ 879 \cdot 488 \bmod 1003 &= 671 \\ 564 \cdot 70 \bmod 1007 &= 207 \\ 218 \cdot 37 \bmod 1009 &= 1003 \end{bmatrix}$$

Il prodotto $23890864094 \times 1883289456$ è ovviamente una soluzione del sistema:

$$\begin{aligned} x &\equiv 739 \pmod{997} \\ x &\equiv 909 \pmod{999} \\ x &\equiv 864 \pmod{1000} \\ x &\equiv 652 \pmod{1001} \\ x &\equiv 671 \pmod{1003} \\ x &\equiv 207 \pmod{1007} \\ x &\equiv 1003 \pmod{1009} \end{aligned}$$

Tutti i conti vengono quindi eseguiti "a pezzi" e poi ricostruiti solo alla fine.

1.9. Potenze Modulo m, Teoremi di Fermat e Eulero

▶ Per calcolare le potenze modulo m

Evaluate $a^n \bmod m$.

Define $a = 2789596378267275$, $n = 3848590389047349$, and $m = 2838490563537459$.

▶ Evaluate

$$a^n \bmod m = 26220\,18141\,09828$$

Il più importante teorema riguardante le potenze modulo m è il cosiddetto *piccolo teorema di Fermat* che dice che, se p è primo e $a \neq 0 \bmod p$, allora

$$a^{p-1} \bmod p = 1$$

Eccone una dimostrazione elementare:
Consideriamo l'insieme

$$Z_p^* = \{1, 2, ..., p-1\}$$

e l'insieme

$$M(a) = \{a \bmod p, 2a \bmod p, ..., (p-1)a \bmod p\}$$

Questi due insiemi coincidono: infatti se prendiamo un qualsiasi $m \in Z_p^*$, *possiamo scriverlo come* $(m \times a^{-1} \times a) \bmod p = (m \times a^{-1})a \bmod p$ *e quindi* $m \in M(a)$. *Allora* $Z_p^* \subseteq M(a)$ *ma* Z_p^* *ha* $p-1$ *elementi distinti e non può essere quindi un sottoinsieme proprio di un insieme con al più* $p-1$ *elementi distinti; deve quindi coincidere con* $M(a)$. *Questo significa che*

$$1 \times 2 \times ... \times (p-1) \bmod p = a \times 2a \times ... \times (p-1)a \bmod p.$$

Raccogliendo otteniamo: $(p-1)! \bmod p = a^{p-1} \times (p-1)! \bmod p$. *Essendo* $(p-1)! \bmod p \neq 0$, *perchè* $(p-1)!$ *ovviamente non contiene* p *come fattore, otteniamo la tesi.*

Il teorema di Fermat fornisce anche un metodo per trovare $a^{-1} \bmod p$: siccome $a^p \bmod n = 1$, si ottiene subito che:

$$a^{-1} \bmod p = a^{p-2} \bmod p$$

Esempio: $p = 17$, $11^{16} \bmod 17 = 1$ e $11^{15} \bmod 17 = 14$ per cui $11^{-1} \bmod 17 = 14$

Dal piccolo teorema di Fermat otteniamo un altro importante risultato: *il teorema di Eulero.*

Se $n = p \times r$ con p e r due numeri primi, poniamo $\varphi(n) = (p-1)(r-1)$ (questa è detta la *funzione di Eulero di n*).

Dal piccolo teorema di Fermat si ottiene che $a^p \bmod p = a \bmod p$ per cui: $a^{\varphi(n)} \bmod p = a^{(p-1)(r-1)} \bmod p = a^{p(r-1)}a^{1-r} \bmod p = a^{r-1}a^{1-r} \bmod p = 1$ e anche:
$a^{\varphi(n)} \bmod r = a^{r(p-1))}a^{1-p} \bmod r = a^{p-1}a^{1-p} \bmod r = 1$. Essendo contemporaneamente $a^{\varphi(n)} \bmod p = 1$ e $a^{\varphi(n)} \bmod r = 1$ (con r e p primi fra loro) si ottiene

$$a^{\varphi(n)} \bmod n = 1$$

Questo è un caso particolare del Teorema di Eulero (è un caso particolare perchè supponiamo che n sia prodotto di due primi).

Il teorema di Eulero (che qui non dimostriamo) dice che se a e n sono primi fra loro, allora:

$$a^{\varphi(n)} \bmod n = 1$$

(anche quando n non è prodotto di due numeri primi). Dove, in questo caso, $\varphi(n)$ è il numero dei numeri $m < n$ e tali che $gcd(m, n) = 1$.

Esempio: $n = 14$, $\varphi(n) = 6$, $11^6 \bmod 14 = 1$

Anche il teorema di Eulero fornisce un metodo per trovare $a^{-1} \bmod n$: siccome $a^{\varphi(n)} \bmod n = 1$, si ottiene subito che:

$$a^{-1} \bmod n = a^{\varphi(n)-1} \bmod n$$

Esempio: $n = 15$, $\varphi(n) = 8$, $11^8 \bmod 15 = 1$ e $11^7 \bmod 15 = 11$ per cui $11^{-1} \bmod 15 = 11$.

▶ Evaluate

$2^{1008} \bmod 1009 = 1$ (Fermat)

$r = 8311$, $p = 2\,738\,497\,289\,527\,589\,233\,333\,433$, $\varphi(n) = 8310 \times 2\,738\,497\,289\,527\,589\,233\,333\,432 = 22\,756\,912\,475\,974\,266\,529\,000\,819\,920$ e $n = 22\,759\,650\,973\,263\,794\,118\,234\,161\,663$

per cui $2^{22\,756\,912\,475\,974\,266\,529\,000\,819\,920} \bmod(22\,759\,650\,973\,263\,794\,118\,234\,161\,663) = 1$ (Eulero)

2. Quadrati modulo p e residui di Gauss

Un caso molto interessante di potenza modulo n è il quadrato; supponiamo di voler risolvere il seguente problema:

Trovare i valori di x per cui $x^2 = 4$ ($mod 7$) cioè risolvere, nel campo Z_7 dei numeri modulo 7, l'equazione $x^2 = 4$. Si ottengono due soluzioni, $x = 2$ e $x = -2 \bmod 7 = 5$. Se invece l'equazione fosse $x^2 = 2$ le soluzioni sarebbero $x = 3$ e $x = -3 \bmod 7 = 4$ infatti $9 \bmod 7 = 16 \bmod 7 = 2$. Ancora, l'equazione $x^2 = 5$ non ha soluzioni (andate a controllare sopra: nella tavola di moltiplicazione modulo 7 il numero 5 non appare sulla diagonale). Naturalmente non dovrebbe essere necessario scrivere tutta la tavola di moltiplicazione, basta ragionare un pò (aiutati da Fermat e Gauss). Limitiamoci al caso in cui n sia un numero primo diverso da 2. (Il caso $n = 2$ è semplicissimo e lasciato al lettore volonteroso, il

caso di n generico è risolto con un sistema di congruenze quando si abbia chiaro cosa succede per i fattori primi di n; per non appesantire troppo il corso faremo solo qualche esempio nel caso generale).

Se l'equazione $x^2 = a \pmod p$ con p *primo dispari* e $a \neq 0 \bmod p$ ammette soluzioni, allora a si dice essere *un residuo di Gauss modulo p*. In questo caso le soluzioni sono sempre due, siano b e $-b$ (quest'ultimo, in realtà, è uguale, $\bmod p$, a $p - b$). Essendo gli elementi di Z_p esattamente $p - 1$ si nota subito che ci sono sempre $(p - 1)/2$ residui e $(p - 1)/2$ non residui (a ogni residuo si associa una coppia di elementi e di coppie ce ne sono $(p-1)/2$). Se a *è un residuo*, si ha $a = b^2$ per cui Fermat ci dice che $a^{(p-1)/2} = b^{p-1} = 1$. Se invece a *non è un residuo*, osservando che (ancora per il teorema di Fermat):

$$(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1) = a^{p-1} - 1 = 0$$

Siccome p è primo, almeno uno dei fattori deve essere uguale a 0, e quindi non essendo a un residuo deve essere $a^{(p-1)/2} = -1 = p - 1$.

Abbiamo ottenuto il più semplice dei criteri di Gauss: per sapere se l'equazione $x^2 = a \pmod p$ ammette soluzioni, si calcola $a^{(p-1)/2}$; se vale 1 ci sono soluzioni, se vale $p - 1$, no.

Esempio: $347^{504} \bmod 1009 = 1$ quindi ci sono interi x per cui $x^2 = 347 \bmod 1009$. *(Trovarli è un'altra storia...provate con* 777 *e* 232*)*

Se poniamo la seguente definizione:

$$[a/p] = a^{(p-1)/2} \bmod p,$$

se a è un residuo modulo p, si ottiene $[a/p] = 1$, mentre se non è un residuo, $[a/p] = -1$.

Ecco invece un "difficile" risultato di Gauss detto *legge di reciprocità:* se $p \neq q$ sono due primi dispari (cioè diversi da 2):

$$[p/q] \times [q/p] = (-1)^{(p-1)/2 \times (q-1)/2}$$

Esempio: siano $p = 7$, $q = 1009$. Siccome $(p - 1)/2 \times (q - 1)/2 = 504 \times 3$ è un numero pari e p e q due primi dispari, $[7/1009] \times [1009/7] = 1$, cioè $7^{504} \bmod 1009 = 1009^3 \bmod 7$; adesso riflettiamo. E' facilissimo **calcolare** che $1009 \bmod 7 = 1$ per cui è immediato **dimostrare** ad esempio che $7^{5040000} \bmod 1009 = 1$ (siete obbligati a calcolarlo su un'isola deserta e potete scegliere tra un libro di algebra o una calcolatrice... attenzione, le batterie prima o poi si esauriscono...)

Altre utili regole di calcolo per i simboli $[a/p]$ sono: (a e b sono interi, p è un primo dispari e p non divide $a \times b$)

$$\begin{aligned} [a \times b/p] &= [a/p] \times [b/p] \\ \left[a^2/p\right] &= [a/p] \times [a/p] = 1 \\ [2/p] &= (-1)^{(p^2-1)/8} \\ [-1/p] &= [p-1/p] = (-1)^{(p-1)/2} \end{aligned}$$

Esempio: 18 è un quadrato perfetto modulo 97 ? Calcoliamo così: $[18/97] = [2/97] \times [9/97] = (-1)^{(97\times 97-1)/8} \times [9/97] = 1$ (perchè 9 è un quadrato). Quindi 18 è un quadrato modulo 97, infatti $42^2 \bmod 97 = 18$. (siamo sulla solita isola...)

La teoria dei residui consente anche di risolvere problemi del tipo:

dimostrare che, per tutti gli interi m, esiste un intero n tale che $n^2 + am^2$ è divisibile per il.numero primo p

Ragioniamo così: se esiste una soluzione di $x^2 = -a \bmod p = (p-a) \bmod p$ posso porre $n = xm$ e quindi ottenere:

$$n^2 + am^2 = x^2m^2 + am^2 = (p - a + a)m^2 = pm^2 = 0 \bmod p$$

Analogamente se avessi da studiare $n^2 - am^2$ cercherei una soluzione di $x^2 = a \bmod p$ per ottenere

$$n^2 + am^2 = x^2m^2 - am^2 = (a - a)m^2 = 0 \bmod p$$

3. Test di primalità

I residui sono uno strumento utile per cercare criteri per verificare se un numero n è primo (sperabilmente un pò più veloci della ricerca di divisori primi fino a $\sqrt{n}$).

Sia q un numero dispari e x un intero positivo minore di q e primo con q. **Se q è primo** già sappiamo che se si calcola $x^{(p-1)/2}$ si ottiene $[x/q]$. Il simbolo $[x/q]$ può essere generalizzato al caso in cui q sia dispari ma non sia primo. Definiamo $[[x/q]]$ essere uguale a $[x/q]$ se q è primo e inoltre imponiamo la proprietà $[[x/q]] \times [[x/q']] = [[x/qq']]$. Si può dimostrare che per $[[x/q]]$ valgono tutte le regole di calcolo valide per $[x/q]$. Allora possiamo dire che se per un numero x come sopra si ha $x^{(q-1)/2} \neq [[x/q]]$ allora q **non può essere primo!** Naturalmente non si può barare, in matematica le difficoltà buttate dalla finestra rientrano sempre dalla porta: si deve riuscire a calcolare in qualche modo $[[x/q]]$ dalle sue proprietà (ovviamente senza sapere i suoi fattori primi!)

Esempio (molto banale): $q = 15$ sia $x = 13$ allora $13^7 \bmod 15 = 7$ mentre (notare che $13 \bmod 15 = -2$)

$$[[13/15]] = [[-1/15]] \times [[2/15]] = (-1)^7 \times (-1)^{(15^2-1)/8} = -1$$

Infatti, come verifica: $15 = 3 \times 5$ per cui:

$$[[13/15]] = [-2/3] \times [-2/5] = [-1/3] \times [2/3] \times [-1/5] \times [2/5] = -1$$

4. Numeri primi molto grandi

▶ La funzione di Maple *nextprime(x)* - rappresentata dal simbolo $p(x)$ - fornisce, per ogni numero x (ragionevolmente grande), il più piccolo numero primo più grande di x. La funzione *isprime(x)* - rappresentata dal simbolo $q(x)$ - determina se x è primo oppure no.

▶ Evaluate

$p(4) = 5$
$p(500) = 503$
$p(8298) = 8311$
$p\,(27384972895275892333333334) = 2738\,497\,289\,527\,589\,233\,333\,433$
$p(10^{45}) = 1000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,009$

▶ Evaluate

$q\,(27384972895275892333333337) = false$
$q(1000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,000\,009) = true$
Infatti:

▶ Factor

$27384972895275892333333337 = 79 \times 34\,664\,522\,652\,247\,964\,978\,903$

5. Il sistema di crittografia di Rivest-Shamir-Adleman (RSA)

Il sistema di crittografia a chiave pubblica di Rivest-Shamir-Adleman (RSA) (è quello con cui è implementato il protocollo SSL, avete presente il lucchetto chiuso che appare quando visitate una pagina Web protetta?) è basato direttamente sul Teorema di Eulero.

Supponiamo che Alice voglia mandare a Bob il numero segreto del suo cellulare $x = 333123456$

Bob genera due numeri primi:

$$q = p(20934) = 20939$$

e

$$r = p\,(259384) = 259387.$$

Poi calcola

$$\begin{aligned} n &= q \times r \\ &= 20939 \times 259387 \\ &= 5431304\,393 \end{aligned}$$

$$\begin{aligned} \varphi(n) &= (q-1) \times (r-1) \\ &= 20938 \times 259386 \\ &= 5431\,024\,068 \end{aligned}$$

A questo punto Bob genera la sua *chiave pubblica* (e, n) dove e è un intero relativamente primo con $\varphi(n)$: ad esempio $e = 1009$ (infatti $\gcd(1009, 5431024068) = 1$) e la sua *chiave privata* (d, n) dove $d = e^{-1} \bmod \varphi(n)$.

$d = 1009^{-1} \bmod 5431\,024\,068 = 4925\,061\,469$.

Sia $x = 333123456$ il testo in chiaro da trasmettere. Messaggi più lunghi di n non sono ammessi per cui bisogna, eventualmente, spezzare il testo in chiaro in frammenti adeguati.

Alice usa la chiave pubblica di Bob per cifrare il messaggio secondo il seguente algoritmo: $y = x^e \bmod n$,

e ottiene $y = 333123456^{1009} \bmod 5431304\,393 = 4978\,962\,229$.

Spedisce a Bob il numero y e *Bob applica la sua chiave privata per riottenere il messaggio in chiaro*:

$$x = y^d \bmod n = 4978\,962\,229^{4925\,061\,469} \bmod 5431304\,393 = 333\,123\,456.$$

Questo metodo funziona per due motivi.

a) se $x^e = y \bmod n$ e $d = e^{-1} \bmod \varphi(n)$, allora $y = x^e + kn$ e $de = 1 - h\varphi(n)$, con h e k numeri interi. Ma allora

$$(x^e + kn)^d = x \cdot (x^{\varphi(n)})^{-h} + m$$

con m un numero intero multiplo di n e, *per il teorema di Eulero*, $x^{\varphi(n)} \bmod n = 1$. Cioè $y^d \bmod n = x$ come si voleva.

b) per ottenere il testo in chiaro non basta avere e,n e y; se non si conoscono q e r l'impresa di invertire la formula di Alice cioè calcolare x da y è quasi disperata perchè la fattorizzazione di numeri molto grandi richiede moltissimo tempo di calcolo.

Ricapitoliamo (in realtà semplificando un po'): ogni sito Web protetto ha un suo numero n (molto grande, non come i nostri esempi) e la corrispondente $\varphi(n)$; quando ci si collega il nostro browser riceve la chiave pubblica del sito, codifica i messaggi e li spedisce. Il sito usa la sua chiave privata per leggere i messaggi ed eseguire le operazioni richieste.

5.1. Esempi di calcolo.

$q = p(444444444444) = 444\,444\,444\,461$

$r = p(555555555555) = 555\,555\,555\,559$

$n = q \times r = 444\,444\,444\,461 \times 555\,555\,555\,559 = 246\,913\,580\,257\,641\,975\,308\,699$

$\varphi(n) = (q-1) \times (r-1) = 555\,555\,555\,558 \times 444\,444\,444\,460 = 246\,913\,580\,256\,641\,975\,308\,680$

$\gcd(777177713, 246\,913\,580\,256\,641\,975\,308\,680) = 1$allora $e = 777177713$ è la chiave pubblica di Bob.

Alice ha il messaggio $x = 12345$, lo codifica $y = 12345^{777177713} \bmod 246\,913\,580\,257\,641\,975\,308\,699 = 102\,530\,308\,001\,854\,922\,814\,302$

Bob usa la sua chiave privata $d = 777177713^{-1} \bmod 246\,913\,580\,256\,641\,975\,308\,680 = 51\,004\,698\,350\,603\,138\,793\,977$ e decodifica il messaggio:

$102\,530\,308\,001\,854\,922\,814\,302^{51\,004\,698\,350\,603\,138\,793\,977} \bmod 246\,913\,580\,257\,641\,975\,308\,699 =$

$12\,345$

$p(123456789987654321) = r = 123\,456\,789\,987\,654\,353$

$p(987654321123456789) = s = 987\,654\,321\,123\,456\,823$

$n = 123\,456\,789\,987\,654\,353 \times 987\,654\,321\,123\,456\,823 = 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519$

$\varphi(n) = (r-1)(s-1) = 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344$

$\gcd(67777777777771, 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344) = 1$

messaggio :8888888888 $y = 8888888888^{67777777777771} \bmod 121\,932\,632\,103\,337\,941\,464\,563\,328\,643\,500\,519 = 78\,687\,260\,944\,075\,815\,618\,371\,573\,626\,229\,331$

$d = 67777777777771^{-1} \bmod 121\,932\,632\,103\,337\,940\,353\,452\,217\,532\,389\,344 = 2604\,717\,670\,245\,025\,077\,664\,852\,739\,463\,811$

$78\,687\,260\,944\,075\,815\,618\,371\,573\,626\,229\,331^{2604\,717\,670\,245\,025\,077\,664\,852\,739\,463\,811} \bmod 121\,932\,63$
$103\,337\,941\,464\,563\,328\,643\,500\,519 = 8888\,888\,888$