DIVISIBILITA'

DEFINIZIONE

a e b interi $a \neq 0$ a <u>divide</u> b se c'è un intero k tale che <u>$b = ak$</u>.

$$a \mid b$$

b è <u>multiplo</u> di a

$3 \mid 15$

$-15 \mid 150$

$7 \mid 21$

PROPOSIZIONE

(1)

<u>per ogni $a \neq 0$, $a \mid 0$ e $a \mid a$.</u> Nonché $1 \mid b$ per ogni b

$0 = a \cdot 0 \Rightarrow k = 0$

$a = a \cdot 1 \Rightarrow k = 1$

$b = 1 \cdot b \Rightarrow k = b$

(2) <u>Se $a \mid b$ e $b \mid c$, allora $a \mid c$</u>

(3) Se $a \mid b$ e $a \mid c$, allora

$$a \mid (sb + tc)$$

per tutti gli interi s e t.

Se $a = 2$, <u>$2 \mid b$</u> significa che b è PARI

NUMERI PRIMI

Un numero $p > 1$ divisibile solo per 1 e se stesso è un <u>numero primo</u>.
Un intero $n > 1$ che non è primo è <u>composto</u>

TEOREMA DEI NUMERI PRIMI

$\pi(x)$ è il numero di primi <u>inferiori</u> a x. Allora

$$\pi(x) \simeq \frac{x}{\ln x}$$

nel senso che:

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$$

Il numero di primi a 100 cifre è

$$\pi(10^{100}) - \pi(10^{99}) \simeq$$

$$\simeq \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \simeq 3{,}9 \times 10^{97}$$

Il setaccio di Eratostene

scegli $n > 2$ intero

$2, 3, 4, \dots, (n-1), n$

PARTO DA 2

PASSO 1 cancella ogni multiplo di 2
e cioè: $4, 6, 8, 10, 12 \dots$

PASSO 2 cancella ogni multiplo di 3
$6, 9, 12, 15, 18, 21$

PASSO 3 cancella ogni multiplo di 5
$10, 15, 20, 25 \dots$

Continua fino al numero primo p e cancella tutti i multipli $2p, 3p, 4p, \dots$

Continua fino al numero p^* più grande ~~di~~ o uguale $\sqrt{n}$ e FERMA. $p^* \geq \sqrt{n}$

I numeri che rimangono sono tutti i primi $2 < p < n$

es $n = 20$ $\sqrt{20} \cong 4.47$ $p^* = 5$

Risultato $(3, 5, 7, 11, 13, 17, 19)$

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Passo 1 ×2				×		×		×		×		×		×		×		×		×
Passo 2 ×3						×			×			×			×			×		
Passo 3 ×5										×					×					×
STOP			3		5		7				11		13				17		19	

The First 1,000 Primes
(the 1,000th is 7919)
For more information on primes see http://primes.utm.edu/

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	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
4001	4003	4007	4013	4019	4021	4027	4049	4051	4057
4073	4079	4091	4093	4099	4111	4127	4129	4133	4139
4153	4157	4159	4177	4201	4211	4217	4219	4229	4231
4241	4243	4253	4259	4261	4271	4273	4283	4289	4297
4327	4337	4339	4349	4357	4363	4373	4391	4397	4409

4421	4423	4441	4447	4451	4457	4463	4481	4483	4493
4507	4513	4517	4519	4523	4547	4549	4561	4567	4583
4591	4597	4603	4621	4637	4639	4643	4649	4651	4657
4663	4673	4679	4691	4703	4721	4723	4729	4733	4751
4759	4783	4787	4789	4793	4799	4801	4813	4817	4831
4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999	5003
5009	5011	5021	5023	5039	5051	5059	5077	5081	5087
5099	5101	5107	5113	5119	5147	5153	5167	5171	5179
5189	5197	5209	5227	5231	5233	5237	5261	5273	5279
5281	5297	5303	5309	5323	5333	5347	5351	5381	5387
5393	5399	5407	5413	5417	5419	5431	5437	5441	5443
5449	5471	5477	5479	5483	5501	5503	5507	5519	5521
5527	5531	5557	5563	5569	5573	5581	5591	5623	5639
5641	5647	5651	5653	5657	5659	5669	5683	5689	5693
5701	5711	5717	5737	5741	5743	5749	5779	5783	5791
5801	5807	5813	5821	5827	5839	5843	5849	5851	5857
5861	5867	5869	5879	5881	5897	5903	5923	5927	5939
5953	5981	5987	6007	6011	6029	6037	6043	6047	6053
6067	6073	6079	6089	6091	6101	6113	6121	6131	6133
6143	6151	6163	6173	6197	6199	6203	6211	6217	6221
6229	6247	6257	6263	6269	6271	6277	6287	6299	6301
6311	6317	6323	6329	6337	6343	6353	6359	6361	6367
6373	6379	6389	6397	6421	6427	6449	6451	6469	6473
6481	6491	6521	6529	6547	6551	6553	6563	6569	6571
6577	6581	6599	6607	6619	6637	6653	6659	6661	6673
6679	6689	6691	6701	6703	6709	6719	6733	6737	6761
6763	6779	6781	6791	6793	6803	6823	6827	6829	6833
6841	6857	6863	6869	6871	6883	6899	6907	6911	6917
6947	6949	6959	6961	6967	6971	6977	6983	6991	6997
7001	7013	7019	7027	7039	7043	7057	7069	7079	7103
7109	7121	7127	7129	7151	7159	7177	7187	7193	7207
7211	7213	7219	7229	7237	7243	7247	7253	7283	7297
7307	7309	7321	7331	7333	7349	7351	7369	7393	7411
7417	7433	7451	7457	7459	7477	7481	7487	7489	7499
7507	7517	7523	7529	7537	7541	7547	7549	7559	7561
7573	7577	7583	7589	7591	7603	7607	7621	7639	7643
7649	7669	7673	7681	7687	7691	7699	7703	7717	7723
7727	7741	7753	7757	7759	7789	7793	7817	7823	7829
7841	7853	7867	7873	7877	7879	7883	7901	7907	7919

end.

A parte 2 tutti i primi sono DISPARI

Si partiscono in due CLASSI

(1) $p \equiv 1 \pmod 4$

(2) $p \equiv 3 \pmod 4$

Per la (1) vale la formula per certi K

$$p = 4K + 1$$

per certi K

$p=$	5	13	17	29	37	41
$K=$	1	3	4	7	8	10

Per la (2) vale la formula per certi K

$$p = 4K + 3$$

$p = 3, 7, 11, 19, 23, 31, 43$

$K = 0\ \ 1\ \ 2\ \ 4\ \ 5\ \ 7\ \ 10$

A parte 2 e 3, tutti i primi DISPARI sono prodotti nella forma

$$p = 6k \pm 1, \quad \text{per certi } k \text{ e certi } \pm$$

e cioè

$$p \equiv \pm 1 \pmod 6$$

solo per certi k e ± 1

$p =$	5	7	11	13	17	19	23	29	31	37
$k =$	1	1	2	2	3	3	4	5	5	6
$\pm =$	$-$	$+$	$-$	$+$	$-$	$+$	$-$	$-$	$+$	$+$

manca $k=4+1$

manca $k=6-1$

$p =$	41,	43,	47
$k =$	7	7	8
$\pm =$	$-$	$+$	$-$

test di primalità di n

provo ~~tutti~~ i numeri

$$(6k \pm 1) \leq \sqrt{n}$$

se n è composto, ad es $n = p \times q$
allora uno dei due, p o q, deve
essere $\leq \sqrt{n}$

NUMERO PRIMO $\boxed{p>0}$

solo 1 e p stesso 'dividono' p

è perfettamente divisibile solo per se stesso e per 1.

$p = 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$

ARITMETICA MODULARE

$\boxed{m \text{ intero} > 0}$

$\boxed{0 \bmod m = 0}$ per definizione

$$a \bmod m = r$$

$\boxed{a \bmod 0 = a}$ per definizione

$$a = k\,m + r$$

$a > 0$ ||
$a < 0$ ||

$$a = \left\lfloor \frac{a}{m} \right\rfloor \cdot m + r$$

$k = \left\lfloor \frac{a}{m} \right\rfloor$

$k \gtrless 0$ ||

$$\underline{0 \le r \le m-1}$$

$\mathbb{Z}_m$ insieme dei residui modulo m

$\boxed{0 \bmod 0 = 0 \text{ per definizione}}$

$|\mathbb{Z}_m| = m$ $\quad 0, 1, 2, \ldots, m-1$

c'è lo zero

CONGRUENZA

$$b \equiv a \pmod m$$

stesso residuo $b \bmod m = a \bmod m = r$

---

teorema generale dell'aritmetica

m intero

$$m = \prod_{i=1}^{n} p_i^{e_i} \qquad e_i > 0 \qquad 1 \le i \le n$$

$m = 60 = 2^2 \cdot 3 \cdot 5$

<u>Teorema</u> ogni intero $n \geq 2$ è prodotto di primi. La fattorizzazione è <u>unica</u>

$$504 = 2^3 \cdot 3^2 \cdot 7$$

$$1124 = 3^? \cdot 5^3$$

$$2 = 1 \cdot 2$$

<u>Lemma.</u> se p è primo e p divide un prodotto di interi $a\,b$, allora $p \mid ab$

allora o: $p \mid a$; oppure: $p \mid b$

Più in generale se $p \mid ab \dots z$

allora p deve dividere uno dei fattori a, b, z.

MASSIMO COMUN DIVISORE

$gcd(a, b) = d$

$mcd(a, b) = d$

è l'intero $d > 0$ più grande che divide sia a che b

$d \mid a$ e $d \mid b$

se $mcd(a, b) = 1$

allora a e b sono "primi tra loro"

o "coprimi"

o "primi relativi"

$mcd(1728, 135)$

$1728 = 2^6 3^2$; $135 = 3^3 5$

$mcd(1728, 135) = 3^2$

$gcd(2^5 3^4 7^2, 2^2 5^3 7) = 2^2 3^0 5^0 7^1 = 2^2 7 = 28$

ALGORITMO DI EUCLIDE

$gcd(482, 1180)$

divido 1180 per 482

dividendo = quoziente divisore + resto

"dividere" dividendo nel divisore

$1180 = 2 \cdot 482 + 216$

quoziente $= 2$
~~resto~~ $= 216$

resto → divisore → dividendo → 1 giro

$\overset{dd}{482} = \overset{q}{2} \cdot \overset{dr}{216} + \overset{r}{50}$

$216 = 4 \cdot 50 + 16$

1 giro

$50 = 3 \cdot 16 + 2$ ← gcd

$16 = 8 \cdot 2 + 0$

ultimo resto ≠ 0

MCD ②

ALGORITMO DI EUCLIDE

$m, n > 0$

$mcd(n, m) =$

$$\frac{0 \le m < n}{mcd(0, n) = n}$$

$mcd(0,0) =$
$=$ indefinito

$mcd(n, n) = n$

$mcd(1, n) = 1$

$mcd(n, m)$
$= mcd(m \bmod n, n)$

ADES.

$mcd(12, 18) =$
$mcd(18 \bmod 12, 12) =$
$mcd(6, 12) =$
$mcd(12 \bmod 6, 6) =$
$mcd(0, 6) = 6$

numeri primi

$mcd(n, m) = 1$

$n \perp m \ ; \ m \perp n$

insieme "ridotto" dei residui   insieme "completo" dei residui (3)

$$\mathbb{Z}^*_m \in \mathbb{Z}_m \rightarrow 0 \div m-1$$

Comprende i residui che sono numeri primi con m

$$p_i \quad 1 \leq i \leq \varphi(m)$$

m intero >0

$$|\mathbb{Z}^*_m| = \varphi(m) \qquad p_i \perp m$$

FUNZIONE FI DI EULERO
FUNZIONE 'TOZIENTE'

X Se $m=p$ è primo allora

$$\varphi(p) = p-1$$

tutti i residui tranne lo 0

$$mcd(0,p) = p.$$

X Se $m = p \cdot q$ con p e q primi allora

$$\varphi(p \cdot q) = (p-1)(q-1)$$

$$\varphi(21) = \varphi(3 \times 7) = (3-1)(7-1) = 2 \times 6 = 12$$

per esempio $m = 6$

$$\mathbb{Z}_6 \equiv [0, 1, 2, 3, 4, 5]$$

quali sono primi con 6 ?

$6 = 2 \times 3$ prodotto di numi primi

0 ? $mcd(0,6) = 6$ — NO

1 ? $mcd(1,6) = 1$ → SI

2 ? $mcd(2,6) = 2$ — NO

3 ? $mcd(3,6) = 3$ — NO

4 ? $mcd(4,6) = 2$ — NO

5 ? $mcd(5,6) = 1$ → SI → $\in \mathbb{Z}_6^*$

$$\varphi(6) = 2 = |\mathbb{Z}_6^*|$$

$$\varphi(6) = \varphi(2 \times 3) = [(2-1)(3-1)] = \underline{2}$$

OK

funzione φ di Eulero per $m = p_1 \times p_2$

NOTAZIONE STINSON

$mcd(a,b)$ $a > b$ $\begin{cases} a = r_0 & r_0 > r_1 \\ b = r_1 \end{cases}$ 5

- $r_0 = q_1 r_1 + r_2$

se $r_2 = 0$ allora $b|a$ e $mcd(a,b) = b$
a è multiplo di b.

se $r_2 \neq 0$ allora

- $r_1 = q_2 r_2 + r_3$

continua finché $r_{n+1} = 0$ allora

$mcd(a,b) = r_n$

- $r_2 = q_3 r_3 + r_4$

$\vdots$

- $r_{n-2} = q_{n-1} r_{n-1} + r_n$
- $r_{n-1} = q_n r_n + 0$ STOP.

n passi dell'algoritmo

$r_0 > r_1 > r_2 \cdots > r_n$

$mcd(12345, 11111) = 1$

dividendo	quoziente	divisore	resto	PASSO
12345 =	1 ·	11111 +	1234	1
11111 =	9 ·	1234 +	5	2
1234 =	246 ·	5 +	4	3
5 =	1 ·	4 +	1	k−1=4
4 =	4 ·	1 +	0	k=5

$mcd(r_0, r_1) = mcd(r_1, r_2) = \dots = mcd(r_{n-1}, r_n) = r_n$

NOTAZIONE STINTSON

- $t_0 = 0$; $t_1 = 1$

- $t_i = t_{i-2} - q_{i-1} t_{i-1}$ $(2 \leq i \leq n)$

essendo $t_i r_1 = r_i$

(a, b) $a = r_0$; $b = r_1$; $a > b$; $r_0 > r_1$

- $s_0 = 1$; $s_1 = 0$

- $s_i = s_{i-2} - q_{i-1} s_{i-1}$ $(2 \leq i \leq n)$

allora si ha

$$0 \leq j \leq n$$

$$\boxed{r_j = s_j r_0 + t_j r_1}$$

s x il più grande
t x il più piccolo

per $j = 0 \rightarrow r_0 = s_0 r_0 + t_0 r_1 = r_0$ $\begin{cases} s_0 = 1 \\ t_0 = 0 \end{cases}$

per $j = 1 \rightarrow r_1 = s_1 r_1 + t_1 r_1 = r_1$ $\begin{cases} s_1 = 0 \\ t_1 = 1 \end{cases}$

---

per $i = n$ $r_n = s_n r_0 + t_n r_1 = \mathrm{mcd}(r_0, r_1)$

Nel TRAPPE gli indici di Euclide (10) sono sbagliati $(a>b)$ poi per Euclide Esteso prende $(b>a)$ e sono

$(b>a)$ $\quad ax_n + by_n = \text{mcd}(a,b)$

$(r_0>r_1)$ $\quad r_1 t + r_0 s_n = \text{mcd}(r_1, r_0)$

quindi

$X \rightarrow t$

$Y \rightarrow s$

X moltiplica il più piccolo
t moltiplica il più piccolo

TRAPPE STINTSON

STINTSON+P $= (a,b)$ ove $a=r_0>b=r_1$ $\quad a>b$

PASSO			
		$0=t_0$ $1=t_1$	$1=s_0$ $0=s_1$
1	$a=r_0=q_1 r_1 + r_2$	t_2	s_2
2	$b=r_1=q_2 r_2 + r_3$	t_3	s_3
3	$r_2 = q_3 r_3 + r_4$	t_4	s_4
	$\vdots \quad \vdots$	$\vdots$	
$n-1$	$r_{n-2} = q_{n-1} r_{n-1} + r_n$	t_n	s_n
n	$r_{n-1} = q_n r_n + 0$	$(-1)^n \frac{r_0}{r_n} = \frac{a}{r_n}$	$(-1)^{n+1} \frac{r_1}{r_n} = \frac{b}{r_n}$

$(-1)^n = \begin{cases} -1 & n \text{ dispari} \\ +1 & \text{pari} \end{cases}$ $\qquad (-1)^{n+1} \begin{cases} -1 & \text{pari} \\ +1 & \text{dispari} \end{cases}$

$t_i \quad s_i$

$(X) \quad (Y)$

$r_0 = a$
$r_1 = b$

$$\begin{cases} r_{n+1} = 0 \\ t_{n+1} = (-1)^n \dfrac{r_0}{r_n} = (-1)^n \dfrac{a}{r_n} \\ s_{n+1} = (-1)^{n+1} \dfrac{r_1}{r_n} = (-1)^{n+1} \dfrac{b}{r_n} \end{cases}$$

ad ogni passo $0 \leq i \leq n$ risulta (11)

$r_0 = a$
$r_1 = b$
$r_0 > r_1$

$$\boxed{s_i r_0 + t_i r_1 = r_i}$$

e per $i = n$

per $i = n$
$a > b$

$$(1) \quad \boxed{s_n a + t_n b = r_n}$$

se prendo (1) mod a, ho

$$t_n b \equiv r_n \pmod{a}$$

se risulta $mcd(a, b) = 1$ e cioè
$$r_n = 1$$

allora

$$t_n b \equiv 1 \pmod{a}$$

$$t_n \equiv b^{-1} \pmod{a}$$

Risulta anche

$r_1 = b$

$$t_i r_1 = r_i \ , \quad 2 \leq i \leq n$$
$$(t_i b = r_i) \pmod{a}$$

ESEMPIO $a=26$, $b=7$ $\quad a=r_0;\ b=r_1 \quad a>b$

$26=2\times 13 \quad mcd(7,26)=1$

		t	s
		0	1
	$r_0 \quad q_1 \quad r_1$	1	0
1	$26 = 3\cdot 7 + 5^{\,r_2}$	$-3^{\,t_2}$	$1^{\,s_2}$
2	$7 = \overset{q_2}{1}\cdot 5 + 2^{\,r_3}$	$4^{\,t_3}$	$-1^{\,s_3}$
	$5 = \overset{q_3}{2}\cdot 2 + 1^{\,r_4}$	$\boxed{-11^{\,t_4}}$	$\boxed{3^{\,s_4}}$
3	$2 = \overset{q_4}{2}\cdot 1 + 0$	$\boxed{26^{\,r_0}}$	$\boxed{-7^{\,-r_1}}$

$n=4$

n pari

$r_4 = r_n = 1$ allora $mcd(26,7)=1$

risulta

$$\begin{cases} s_4 = 3 \\ t_4 = -11 \end{cases} \qquad s_4 a + t_4 b = 1 = r_4 \leftarrow \text{passo } 3$$

$$3\times 26 + (-11)\times 7 = 1 \leftarrow \Delta = 11\times 7 - 3\times 26 = -1$$

infatti $\quad 78 - 77 = 1$

risulta anche

$$(-11)\times 7 \equiv 1 \pmod{26}$$

$$15\times 7 \equiv 1 \pmod{26}$$

allora $\quad b^{-1} \equiv 7^{-1} \equiv 15 \pmod{26}$

Si ha anche che $\quad a^{-1} \equiv 26^{-1} \equiv 3 \pmod 7$

ma risulta anche (13)

$$s_3 a + t_3 b = 2 = r_3 \leftarrow \text{resto 2}$$

$$(-1)\,26 + 4 \times 7 = 2$$
$$-26 + 28 = 2$$

$$s_2 a + t_2 b = 5 = r_2$$

$$1 \times 26 + (-3) \times 7 = 5$$
$$26 - 21 = 5$$

E inoltre

$$t_i\, r_1 = r_i$$

esempio $\quad t_3\, r_1 = r_3 \pmod{r_0}$

$$t_3 = 4;\ r_1 = 7;\ r_3 = 2 \Rightarrow 4 \times 7 \equiv 2$$
$$28 \equiv 2 \pmod{26}$$

oppure $\quad t_2\, r_1 = r_2 \pmod{r_0}$

$$t_2 = -3;\ r_1 = 7;\ r_2 = 5$$

$$(-3) \times 7 \equiv 5$$
$$-21 \equiv 5 \pmod{26}$$

$\mathrm{mcd}(\overset{a}{105},\overset{b}{72}) = \mathrm{mcd}(72,105)$

	$a = q_1 \times b + r_2$		
		0	1
		1	0
1	$105 = 1 \cdot 72 + 33$	-1^{t_2}	1^{s_2}
2	$72 = 2 \cdot 33 + 6^{r_3}$	3^{t_3}	-2^{s_3}
3	$33 = 5 \cdot 6 + 3^{r_4}$	-16^{t_4}	11^{s_4}
4	$6 = 2 \times 3 + 0$	35	-24

$n=4$

$\frac{a}{r_4} = \frac{105}{3} \qquad -\frac{72}{3} = \frac{-b}{r_4}$

$b\,t_4 + a\,s_4 = r_4 \quad b<a$

$72(-16) + 105 \cdot 11 = 3$

$72(-1) + 105 \cdot 1 = 33$

$72 \times 3 + 105(-2) = 6$

TRAPPE $a x_i + b y_i = r_i$ se $a<b$

$x \to t$

$y \to s$

ultimo quadrato

$-16(-24) - 11 \times 35 = 1$

$384 - 385 = -1$ (n fondi)

$mcd(1180, 482)$ $\quad 1180 = a = r_0$
$\quad 482 = b = r_1$

(15)

$a > b$
$r_0 > r_1$

		$t = y$	$s = x$
		0	1
		1	0
1	$1180 = 2 \cdot 482 + 216^{r_2}$	-2^{t_2}	1
2	$482 = 2 \cdot 216 + 50^{r_3}$	5	-2
3	$216 = 4 \cdot 50 + 16^{r_4}$	-22	9
4	$50 = 3 \cdot 16 + 2^{r_5}$	71	-29
	$16 = 8 \cdot 2 + 0$	-590	241

$n = 5$

$\frac{1180}{2} = 590$

$\frac{482}{2} = 241$

se $a > b$

t modifica il più piccolo

$$\boxed{b \times t_5 + a \times s_5 = r_5}$$

(1) $482 \times 71 + (-29)\,1180 = 2$

$34222 - 34220 = 2$

se ometto l'ultimo quadrato e divido x 2

n dispari $= 1$

n pari $= -1$

$$\boxed{\begin{array}{c} 241 \times 71 - 29 \times 590 = 1 \\ 17111 - 17110 = 1 \end{array}}$$

$\det \begin{vmatrix} t_n & s_n \\ t_{n+1} & s_{n+1} \end{vmatrix} = t_n \cdot s_{n+1} - s_n t_{n+1} = -1^{n+1}$

n pari o dispari (1) $\boxed{t_n \cdot s_{n+1} - s_n t_{n+1} = -1^{n+1}}$ $\quad (-1)^{n+1}$

infatti $t_n = b^{-1}$ mod a $\quad t_{n+1} = \frac{a}{r_n}(-1)^n$; $\quad s_n = a^{-1}$ (mod b) $\quad s_{n+1} = \frac{b}{r_n}(-1)^{n+1}$

per dimostrare la (1)

$$\begin{cases} s_{n+1} = \dfrac{b}{r_n}(-1)^{n+1} \\ t_{n+1} = \dfrac{a}{r_n}(-1)^{n} \end{cases}$$

$$(-1)^{n+1} t_n \times b - (-1)^n s_n \times a = r_n (-1)^{n+1}$$

$$(-1)^{n+1}(t_n b - s_n a) = r_n (-1)^{n+1}$$

$$t_n b - s_n a = r_n$$ c.v.d

mcd(33, 12)

		0	1
		1	0
1	$33 = 2 \times 12 + 9$	-2	1
2	$12 = 1 \times 9 + 3$	3	-1
$n = 3$	$9 = 3 \times 3$	-11	4

dispari

$(-1)^3 =$

$3 \times 4 - (-1)(-11) = 12 - 11 = 1$

n dispari

$$3 \times 12 + (-1)33 = 3$$

$$36 - 33 = 3$$

$$-2 \times 12 + 1 \times 33 = 9$$

$$\frac{33}{12} = 2 + \cfrac{1}{1 + \cfrac{1}{3}} = 2 + \frac{3}{4} = \frac{11}{4}$$

Frazioni Continue

Algoritmo di EUCLIDE

$\mathrm{mcd}(a,b)$ $a>b$

$a=r_0$
$b=r_1$ $r_0>r_1$

$$\begin{cases} r_0 = a = q_1 b + r_2 \\ r_1 = b = q_2 r_2 + r_3 \\ r_2 = q_3 r_2 + r_4 \\ \vdots \\ r_{n-2} = q_{n-1} r_{n-1} + r_n \\ r_{n-1} = q_n r_n + 0 \end{cases}$$

n passi

$r_0 > r_1 > r_2 > \dots$
$\dots > r_{n-1} > r_n$

$\mathrm{mcd}(a,b) = r_n$ $(a>b)$

STOP $\boxed{r_{n+1}=0}$

---

posso scrivere

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\dots + \cfrac{1}{q_n}}}}$$

Infatti
$a>b$

$$a = q_1 b + r_2 \quad (0 \le r_2 < b)$$

$$\frac{a}{b} = q_1 + \frac{r_2}{b} \quad \left(0 \le \frac{r_2}{b} < 1\right)$$

Congruenze

Definizione

Siano a, b, n interi con $n \neq 0$. Si dice che

$$a \equiv b \pmod{n}$$

se $a-b$ è multiplo (positivo o negativo) di n e cioè $n \mid (a-b)$

n divide $(a-b)$

$$a \equiv b \pmod{n}$$

se a e b differiscono per un multiplo di n.

$$a = b + kn \quad (k \text{ intero positivo o negativo})$$

Es.

$$32 \equiv 7 \pmod{5}$$

$$5 \mid (32-7) = 5 \mid 25$$

$$25 = 5 \times \underline{5}$$

oppure

$$32 = 7 + \underline{5} \times 5 \quad k = 5$$

Proposizione

Siano a, b, c, n interi con $n \neq 0$

(1) $a \equiv 0 \pmod{n}$ se e solo se $n \mid a$

(2) $a \equiv a \pmod{n}$

(3) $a \equiv b \pmod{n}$ se e solo se $b \equiv a \pmod{n}$

(4) Se $a \equiv b$ e $b \equiv c \pmod{n}$ allora $a \equiv c \pmod{n}$.

Gli interi modulo n $(\mathrm{mod}\ n)$ sono appartenenti all'insieme $\mathbb{Z}_n \equiv \{0, 1, 2 \dots n-1\}$

$$a \equiv r \pmod{n}$$

$$a = n \cdot q + r \quad (0 \leq r < n)$$

r = resti = residui $\quad \underline{0 \leq r < n}$

Proposizione

a, b, c, d, n interi con $n \neq 0$, e supponiamo

$$a \equiv b \pmod n \qquad c \equiv d \pmod n$$

Allora

$$a + c \equiv b + d, \quad a - c \equiv b - d,$$

$$ac \equiv bd \pmod m$$

addizione, sottrazione e moltiplicazione OK!

Attenzione alla divisione

$a \cdot b \pmod n$

se $a \cdot b < n$ OK $a \cdot b \pmod n = ab$

se $a \cdot b > n$ allora

$$a \cdot b = \left\lfloor \frac{a \cdot b}{n} \right\rfloor \times n + r$$

$$r = a \cdot b - \left\lfloor \frac{ab}{n} \right\rfloor \times n$$

$$ab \pmod n = r$$

$\times$ mod 6 Tabelle di addizione $\pmod 6$

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

Tabella di moltiplicazione mod 6

$\times$	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

Risolvere

$$x+7\equiv 3 \pmod{17}$$

$$x\equiv 3-7\equiv -4\equiv 13 \pmod{17}$$

DIVISIONE

Si può dividere per $a \pmod n$ se $\mathrm{mcd}(a,n)=1$ e cioè se $a\perp n$.

<u>Proposizione</u> Siano a, b, c, n interi con $n\neq 0$ e con $\gcd(a,n)=1$. Se $ab\equiv ac \pmod n$, allora $b\equiv c \pmod n$. Se $a\perp n$ possiamo dividere ambedue i lati della congruenza per a.

Esempio $\quad 2x+7 \equiv 3 \pmod{17}$

$$2x \equiv 3-7 \equiv -4 \quad \text{allora se divido per } 2 \perp 17$$

$$(\bmod 17) \qquad x \equiv -2 \equiv 15$$

<u>Proposizione</u>

supponiamo $mcd(a,n)=1$ $(a<n)$ siano s e t interi tali che $at + ns = 1$ che si individuano con l'algoritmo di Euclide esteso. Allora $at \equiv 1 \pmod n$ allora s è il moltiplicatore inverso di a mod n $\quad t \equiv a^{-1} \pmod n$

$a<n$

$$11111\,x \equiv 4 \pmod{12345}$$

	n		q	a		r		t	s
								0	1
								1	0
1	12345	=	q_1 1 ·	11111	+	1234	r_2	-1	1
2	11111	=	q_2 9 ·	1234	+	5	r_3	10	-9
3	1234	=	q_3 246 ·	5	+	4	r_4	-2461	2215
4	5	=	q_4 1 ·	4	+	1	r_5	2471	-2224
5	4	=	q_5 4	1	+	0		~~12345~~	11111

$n=5$

da questo si ha

$$11111 \times 2471 - 12345 \times 2224 = 1$$

e cioè $\quad 11111 \times 2471 \equiv 1 \pmod{12345}$

e cioè $\quad 2471 \equiv (11111)^{-1} \pmod{12345}$

allora

$$X \equiv 4 \times 2471 \equiv 9884 \pmod{12345}$$

Procedura per risolvere la congruenza del tipo

$$ax \equiv b \pmod{n}$$

quando $mcd(a,n) = d > 1$

1. se $d \nmid b$ non c'è soluzione
2. se $d \mid b$ allora considera la nuova congruenza

$$\left(\frac{a}{d}\right) x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{n}{d}\right)$$

$\frac{a}{d}$; $\frac{b}{d}$ e $\frac{n}{d}$ sono interi e

$$mcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$$

e si risolve con l'algoritmo di Euclide esteso e si ottiene la soluzione x_0.

3. le soluzioni sono allora nel numero di "d"

$$x_0;\ x_0 + \frac{n}{d};\ x_0 + 2\left(\frac{n}{d}\right);$$

$$\dots\ x_0 + (d-1)\frac{n}{d}.$$

Per esempio $12x \equiv 21 \pmod{39}$ (1)

$mcd(12,39) = 3$ che divide 21. La (1) diventa $4x \equiv 7 \pmod{13}$

$x_0 = 5$: le tre soluzioni sono $x \equiv 5, 18, 31 \pmod{39}$

Piccolo Teorema di FERMAT

se p è primo, e p non divide a e cioè a non è multiplo di p, allora

$$a^{p-1} \equiv 1 \pmod{p}$$

$\mathrm{mcd}(a,p)=1$

$a \in \mathbb{Z}_p^*$

$a \perp p$

Sia $\mathbb{Z}_p^* = \{1,2,3,\dots,p-1\}$

Si consideri l'insieme ottenuto con la mappatura

$$\gamma(x) = ax \pmod{p} \qquad x \in \mathbb{Z}_p^*$$

Ad es. $\begin{cases} p=7 \\ a=2 \end{cases}$ $\quad 2 \perp 7$

$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$

riottengo gli stessi numeri $\in \mathbb{Z}_p^*$

$$\begin{cases} \gamma(1) = 1\times 2 = 2 \mod 7 \\ \gamma(2) = 2\times 2 = 4 \\ \gamma(3) = 3\times 2 = 6 \\ \gamma(4) = 4\times 2 = 8 \mod 7 = 1 \\ \gamma(5) = 5\times 2 = 10 \mod 7 = 3 \\ \gamma_6 = 6\times 2 = 12 \mod 7 = 5 \end{cases}$$

Allora posso scrivere

$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv (a \cdot 1)(a \cdot 2)(a \cdot 3) \cdots [a(p-1)]$$

$$(p-1)! \equiv a^{p-1}(p-1)! \pmod p$$

e quindi

$$1 \equiv a^{p-1} \pmod p$$

---

questo lega l'esponente <u>(p−1) modulare</u> al <u>modulo p</u>.

Ad es. $p = 11$ $\quad 3 \perp 11$

prendiamo $3^{10} \equiv 1 \pmod{11}$

$$3^{53} \equiv (3^{10})^5 \cdot 3^3 \equiv 5 \pmod{11}$$

$$\begin{cases} 53 \equiv 3 \pmod{10} & \leftarrow \text{esponenti} \\ 3^{53} \equiv 3^3 \pmod{11} \end{cases}$$

Usualmente se $2^{n-1} \equiv 1 \pmod{n}$ allora

n è primo.

Ma non sempre $560 = 3 \cdot 11 \cdot 17$ ma

$$2^{560} \equiv 1 \pmod{561}$$

ma queste eccezioni sono rare

Pertanto se $2^{n-1} \equiv 1 \pmod{n}$ allora molto probabilmente n è primo.

~~Eccezioni~~ Questo è un modo per cercare i numeri primi usando $2(n-1)$ passi di calcolo per ogni esponenziale modulare.

Si fa così: scegli un punto di partenza n_0 e testa tutti i numeri DISPARI

$$n \geq n_0$$

~~e~~ e controlla se

$$2^{n-1} \equiv 1 \pmod{n}.$$

Se n fallisce, scarta e va avanti. Se n passa il test, allora va effettivamente verificato se n è primo (primality test).

ict CONSULTING

TEOREMA DI EULERO

$\phi(n) = |\mathbb{Z}_n^*|$ funzione ϕ di Eulero

se p è primo

Se $n = p^r$ allora dobbiamo eliminare dalla lista tutti gli interi da 0 a $(n-1)$ di $\mathbb{Z}_n$ ciascun numero p-esimo (kp) $k = 0, 1, (p^{r-1})$

$n = p^r$

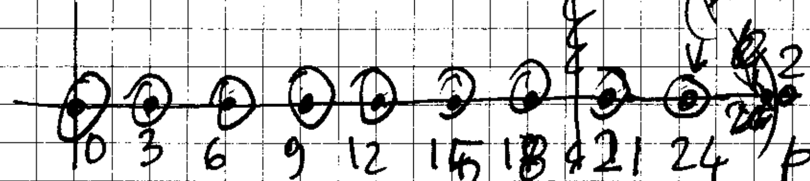
$$\phi(p^r) = \left(1 - \frac{1}{p}\right)p^r = p^r - p^{r-1} \quad k = 0, 1 \dots (p^{r-1})$$

es $p = 3$

$r = 3$

$p^{r-1} = 3^2 = 9$

$3^2 - 1 = 8$



$$p^r - \frac{p^r}{p} = p^r - p^{r-1}$$

cioè $27 - 9 = p^r\left(1 - \frac{1}{p}\right) = 27\left(1 - \frac{1}{3}\right)$

$p^r - p^{r-1}$

$$\boxed{\phi(n) = n \prod_{\forall i \; p_i | n} \left(1 - \frac{1}{p_i}\right)}$$

che dividono n

se m primi distinti $1 \le i \le m$

$$\phi(n) = \prod_{i=1}^{m} \left(p_i^{r_i} - p_i^{r_i - 1}\right) = \prod_{i=1}^{m} p_i^{r_i} \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

$$n = \prod_{i=1}^{m} p_i^{r_i}$$

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

7^{803} quali sono le ultime 3 cifre decimali? Risposta: 343.

$1000 = 2^3 \times 5^3$

$\varphi = (2^3 - 2^2) \times (5^3 - 5^2) = 4 \times 100 = 400$

basta fare $7^{803} \bmod 1000$

ma $\phi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$

$7^{400} \equiv 1 \pmod{1000}$ $\quad 7^{803} \equiv (7^{400})^2 \, 7^3 \equiv 7^3 \equiv 343 \pmod{1000}$

abbiamo concluso da 803 a 3 perché verificato

$\underline{803 \equiv 3 \ [\bmod \varphi(1000)]}$ $\pmod{400}$

PRINCIPIO BASE

Siano a, n, x, y interi $\mathrm{mcd}(a, n) = 1$, $n \geq 1$

Se (1) $x \equiv y \pmod{\varphi(n)}$

Allora

(2) $a^x \equiv a^y \pmod{n}$.

Se si vuole lavorare con esponenziali mod n, bisogna lavorare mod $\phi(n)$ tra gli esponenti

da (1) $x = y + \phi(n) k$ allora (2) $a^x = a^{y + \varphi(n) k} = a^y \left(a^{\varphi(n)}\right)^k \equiv a^y 1^k \equiv a^y \pmod{n}$

Teorema di Lagrange

$m > 0$

prendo un $a \perp m$

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

$$\frac{a \perp m}{m > 0}$$

si applica per $a \in \mathbb{Z}_m^*$

Fermat

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

---

ove $\varphi(m) = \prod_{i=1}^{n} \left(p_i^{l_i} - p_i^{l_i - 1}\right)$

$m = 60$

$60 = 2^2 \cdot 3 \cdot 5$

$\varphi(60) = (2^2 - 2^1)(3-1)(5-1) = 16$

Fermat $\varphi(p) = (p-1)$

Esponenziali modulari $\quad x^q \pmod n$

$2^{1234} \bmod (789)$

potenze consecutive di 2 modulo 789
1233 volte consecutive

oppure

$$2^2 \equiv 4 \pmod{789}$$

$$2^4 \equiv 4^2 \equiv 16$$

$$2^8 \equiv 16^2 \equiv 256$$

$$2^{16} \equiv 256^2 \equiv 49$$

$$2^{32} \equiv 34$$

$$2^{64} \equiv 367$$

$$2^{128} \equiv 559$$

$$2^{256} \equiv 37$$

$$2^{512} \equiv 580$$

$$2^{1024} \equiv 286$$

$1234 = 1024 + 128 + 64 + 16 + 2$

$\equiv (10011010010)$ $\quad$ allora

11 BIT

$$2^{1234} = 286 \cdot 559 \cdot 367 \cdot 49 \cdot 4 \equiv 481 \pmod{789}$$

Col Square & Multiply per calcolare

$$a^k \pmod{n}$$

servono al massimo $2 \log_2(k)$
moltiplicazioni mod n
e il numero più grande con cui
lavoro non supera mai n^2

Se a, k e n sono numeri a 100 cifre decimali

(a^k) ha più di 10^{100} cifre decimali (*)
ma bastano $2 \cdot \log_2(k) = 700$ STEP

il numero più grande ha 200 cifre decimali
(n^2)

$$^{*}\ 2^{350} \cong 2{,}3 \ 10^{105}$$

Calcolo di esponenziali modulari
del tipo
$$x^b \bmod m.$$
Due metodi
- square and multiply
- Euclide esteso, che vale solo se l'esponenziale si riferisce ad una inversione

m è primo, m ha k bit
$$k = \lfloor \log_2 m \rfloor + 1$$
l'addizione di due interi si fa in tempo $O(k)$, ma la moltiplicazione richiede $O(k^2)$.

Ora la riduzione modulo m di un esponenziale può essere ridotta quella di moltiplicazioni successive
$$x \qquad x, y \in \mathbb{Z}_m \quad (0 \le x, y \le m-1)$$
$$xy \bmod m$$
faccio prima xy (un intero a $2k$ bit)
e poi riduco modulo m
Se $x^b \bmod m$ allora ho $(b-1)$ moltiplicazioni da fare
$$\left.\begin{array}{l} \bullet\ x \cdot x = x^2 \\ \bullet\ x^2 x = x^3 \\ \bullet\ x^{b-1} x = x^b \end{array}\right\} b-1 \text{ moltiplicazioni}$$

SQUARE & MULTIPLY

riduce invece il numero delle moltiplicazioni a 2ℓ, ove

$$\ell = \lfloor \log_2 b \rfloor + 1$$

è il numero di bit di b (esponente).

In realtà il numero di moltiplicazioni è 'ℓ' se b è fatto di tutti bit=0, mentre è '2ℓ' soltanto se b è composto da tutti bit = 1.

Posso ~~infatti~~ porre b in notazione binaria

$$b = \sum_{i=0}^{\ell-1} b_i 2^i$$

ove

$$b_i = \begin{cases} 0 \\ 1 \end{cases} ; \quad 0 \leq i \leq \ell - 1$$

e calcolare sequenzialmente

$$z = x^b \bmod m$$

1. $z = 1$
2. per $i = \ell - 1$ fino a 0, esegui
3. $z = z^2 \bmod m$ ← 'ℓ' quadrature
4. se $b_i = 1$ allora $z = z x \bmod m$ ← 'a' moltiplicazioni $0 \leq a \leq \ell$

(B) $b_i = \begin{cases} 0 \\ 1 \end{cases} ; 0 \leq i \leq \ell-1$

CEFRIEL

SQUARE & MULTIPLY

$$x^b \bmod m = \left(x^{\sum_{i=0}^{\ell-1} b_i 2^i} \right) \bmod m =$$

$$x^b \bmod m = \left\{ \prod_{i=0}^{\ell-1} \left[\left(x^{b_i 2^i} \right) \bmod m \right] \right\} \bmod m$$

la produttoria contiene tanti termini, da 0 a ℓ, quanti sono i $b_i = 1$ $(0 \leq i \leq \ell-1)$

$(q) = (q) \bmod m$

Esempio

$\ell = 5$ $b = 31$ $\quad (x^{31}) = \underset{b_0}{(x)} \underset{b_1}{(x^2)} \underset{b_2}{(x^4)} \underset{b_3}{(x^8)} \underset{b_4}{(x^{16})}$

$b = 29$ $\quad (x^{29}) = (x)(x^4)(x^8)(x^{16})$

S&M

0. $z = 1$
1. per $i = \ell-1$ fino 0
2. $z = z^2 \bmod m$
3. se $b_i = 1$ allora $z = zx \bmod m$

	b_0	b_1	b_2	b_3	b_4
31	1	1	1	1	1
29	1	0	1	1	1

	$z = 1$		$z = 1$	
b_4	$1^2 x = x$	1	$1^2 x = x$	1
b_3	$x^2 x = x^3$	1	$x^2 x = x^3$	1
b_2	$x^6 x = x^7$	1	$x^6 x = x^7$	1
b_1	$x^{14} x = x^{15}$	1	x^{14}	0
b_0	$x^{30} x = \underline{x^{31}}$	1	$x^{28} x = \underline{x^{29}}$	1

SQUARE & MULTIPLY x esponenziali

↳ $7^{11} \bmod 26$

prendo l'esponente e lo metto in binario

1011

PARTO SEMPRE DA 1 → 1

SQUARE & MULTIPLY	1	$1^2 \times 7 \equiv 7$
SQUARE	0	$7^2 \equiv 23$
SQUARE & MULTIPLY	1	$23^2 \times 7 \equiv 11$
SQUARE & MULTIPLY	1	$11^2 \times 7 \equiv 15$

mod 26

RISULTATO FINALE

$$7^{11} \bmod 26 = 15$$

(9)

$2^{\frac{466}{2}} = 2^{233} \mod 467 = 466 \neq 1 \quad \ell = 8$

233   1 1 1 0 1 0 0 1

255   128 64 32 16 8 4 2 1

22

1	$1^2 \times 2 \equiv 2 \mod 467$
1	$2^2 \times 2 = 8$
1	$64 \times 2 = 128$
0	$(128)^2 = 39 \mod 467$
1	$39^2 \times 2 = 240 \mod 467$
0	$(240)^2 = 159$
0	$(159)^2 = 63$
1	$(63)^2 \times 2 = 466 \neq 1$ OK

$16384 - 128^2$
16345
39

3042
2802
240

57600
57441
159

25281
25218
63

7938
7472
466

$2^{\frac{466}{233}} = 2^2 = 4 \mod 467 = 4 \neq 1$ OK

2 e' primitivo di $\mathbb{Z}^*_{467}$

Sugli elementi primitivi di $\mathbb{Z}_p^*$ con p primo > 0

Fermat afferma: se $a \in \mathbb{Z}_p^*$, allora

$$a^{p-1} \equiv 1 \pmod{p}$$

e cioè un caso particolare di Lagrange: se $a \in \mathbb{Z}_m^*$ (m intero >0), allora

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

L'ordine di un elemento è l'intero $n > 0$ <u>più piccolo</u> tale che

$$a^n \equiv 1 \pmod{m}$$

Un elemento $\alpha \in \mathbb{Z}_p^*$ <u>ha ordine $p-1$</u>

$$\alpha^{p-1} \equiv 1 \pmod{p}$$

è <u>primitivo</u>, se e solo se, genera tutti gli elementi di $\mathbb{Z}_p^*$ $(1; 2; \ldots; p-1)$

$$\{\alpha^i : 1 \leq i \leq p-1\} = \mathbb{Z}_p^*$$

ogni elemento $\beta \in \mathbb{Z}_p^*$ si esprime come

$$\beta = \alpha^i \quad ; \quad 1 \le i \le p-1$$

l'ordine di β è

$$\beta^{\frac{p-1}{\mathrm{mcd}(p-1,\, i)}} \equiv 1 \pmod p$$

e cioè β può avere ordine sottomultiplo di $p-1$; se

$$\mathrm{mcd}(p-1,\, i) = 1$$

e cioè se $i \perp (p-1)$, allora l'ordine di β è <u>esattamente</u> $p-1$ ed è anche lui un elemento primitivo: $\beta^{p-1} \equiv 1 \pmod p$

Allora tutti gli i $(1 \le i \le p-1)$ che sono primi con $(p-1)$ sono esattamente:

Numero di elementi primitivi di $\mathbb{Z}_p^*$ $= \varphi(p-1)$

Poiché $p-1 = \prod_{i=1}^{n} q_i$; q_i primi > 0 $\quad \alpha \in \mathbb{Z}_p^*$

α è <u>primitivo</u>, se e solo se

$(1 \le i \le n)$ $\quad \alpha^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p \quad \forall i$

per <u>tutti</u> gli indici i.

Se α è una radice primitiva di $\mathbb{Z}_p^*$, p primo > 0, allora

Per n intero > 0 :

1 $\begin{cases} \alpha^n \equiv 1 \pmod p, \text{ se e solo se} \\ n \equiv 0 \pmod{p-1} \end{cases}$

Per j, k interi > 0 :

2 $\begin{cases} \alpha^j \equiv \alpha^k \pmod p, \text{ se e solo se} \\ j \equiv k \pmod{p-1} \end{cases}$

Infatti 1 se $n \equiv 0 \pmod{p-1}$, allora

$n = (p-1)m$, per certi interi m

allora si ha $\alpha^n \equiv (\alpha^m)^{p-1} \equiv 1 \pmod p$

applicando il teorema di Fermat
(se $\alpha \in \mathbb{Z}_p^*$ e m intero, anche $\alpha^m \in \mathbb{Z}_p^*$)
anche $\alpha^m \bmod p \in \mathbb{Z}_p^*$, se $\alpha \in \mathbb{Z}_p^*$

2 si assume $j \geq k$

$$\alpha^j \equiv \alpha^k \pmod p$$

$$\alpha^{j-k} \equiv 1 \pmod p$$

Dallo 1 si ha che quest'ultima è vera se

$$j-k \equiv 0 \pmod{p-1}$$

e cioè se

$$j \equiv k \pmod{p-1}.$$

Nella formula della firma di ElGamal

$$\alpha^P \equiv \alpha^{k\delta + a\gamma} \pmod p$$

α primitivo di $\mathbb{Z}_p^*$ è vera se

$$P \equiv k\delta + a\gamma \pmod{p-1}.$$

Esempio $p=7$ $\quad \mathbb{Z}_7^* \equiv \{1; 2; 3; 4; 5; 6\}$

$p-1=6=2\times 3$

$\varphi(6)=1\times 2=2$ ha due elementi primitivi

Fermat $a\in \mathbb{Z}_7$ $\quad a^6\equiv 1 \pmod 7$

$\boxed{\text{Vediamo se 6 è primitivo.}}$

$$\begin{cases} 6^{\frac{6}{2}}\not\equiv 1 \ ? & 6^3\equiv 216\equiv 6 \pmod 7 \quad \text{ok} \\ 6^{\frac{6}{3}}\not\equiv 1 \ ? & 6^2\equiv 36\equiv 1 \quad \text{NO!} \end{cases}$$

6 NON è primitivo, ma applicando Fermat, si ha che $6^6\equiv 1 \pmod 7$

$6^6\equiv 46656\equiv 1 \pmod 7$

ma l'ordine di 6 è 2 (l'esponente più piccolo) tale che $6^2\equiv 1 \pmod 7$ $\quad$ 6 ha ordine 2

$\boxed{\text{Vediamo se 2 è primitivo}}$ $\quad$ 2 ha ordine 3

$2^3\not\equiv 1 \pmod 7$ $\quad 8\equiv 1$ NO!

$\boxed{\text{Vediamo se 3 è primitivo}}$

$$\begin{cases} 3^3\equiv 27\equiv 6 \pmod 7 \\ 3^2\equiv 9\equiv 2 \pmod 7 \end{cases}$$ Si! 3 è primitivo

(6)

l'ordine di 3 è $p-1$

$$729 \equiv 3^6 \equiv 1 \pmod 7$$

Ora verifichiamo la proprietà

$$\begin{cases} 3^4 \equiv 3^{x+1} \pmod 7 \\ 4 \equiv x+1 \pmod 6 \end{cases}$$

l'ultima equazione dice che

$$4 = 6m + x + 1, \quad m \text{ intero}$$

e cioè

$$x = 3 - 6m$$

per $m=0 \rightarrow x=3$
$m=-1 \rightarrow x=9$
$m=-2 \rightarrow x=15$

infatti

$$3^4 \equiv 3^{10} \equiv 3^{16} \equiv 4 \pmod 7$$

$$4 \equiv 10 \equiv 16 \pmod 6$$

L'altro elemento primitivo $\in \mathbb{Z}_7^*$ è 5

$$\begin{cases} 5^3 \equiv 125 \equiv 6 \pmod 7 \\ 5^2 \equiv 25 \equiv 4 \pmod 7 \end{cases}$$

$n > 0$ minimo!
$1^1 \equiv 1$
$1^2 \equiv 1$
$1^3 \equiv 1$
1 è di ordine 1

---

4 ha ordine 3 $\quad 4^3 \equiv 64 \bmod 7 = 1$; $4^2 \equiv 16 = 2$ ok

ESEMPIO $p=11$

$$\mathbb{Z}_{11}^* \equiv \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}; \quad |\mathbb{Z}_{11}^*| = 10$$

$\varphi(10) = \varphi(5\times 2) = 4$ elementi primitivi di

$ord(\alpha) =$ "ordine" 10

gli altri hanno ordine

$$ord(\beta) = \frac{10}{mcd(10, i)} \qquad 1 \le i \le p-1$$

deve essere $\alpha^{\frac{10}{5}}$; $\alpha^{\frac{10}{2}}$ e cioè α^2 ed $\alpha^5 \not\equiv 1$ mod 11

es

2 $\begin{cases} 2^2 \equiv 4 \not\equiv 1 \pmod{11} \\ 2^5 \equiv 64 \equiv 9 \not\equiv 1 \text{ ok} \end{cases}$ $\quad 2^{10} \equiv 1024 \equiv \underline{1}$ ok Fermat

$\begin{cases} 3^2 \equiv 9 \not\equiv 1 \pmod{11} \\ 3^5 \equiv 243 = 1 \ \underline{\text{NO}} \end{cases}$ $\quad$ 3 è di ordine 5 $= \frac{10}{\cancel{2}} = 5$

$\begin{cases} 5^2 \equiv 25 \equiv 3 \not\equiv 1 \\ 5^5 \equiv 3125 = 1 \text{ NO} \end{cases}$ $\quad$ 5 è di ordine 5

7 $\begin{cases} 7^2 \equiv 49 \equiv 5 \not\equiv 1 \\ 7^5 \equiv 16807 \equiv 10 \not\equiv 1 \ \underline{\text{ok}} \end{cases}$ $\quad 7^{10} \equiv 1$ ok

797

$4^2 \equiv 16 \equiv 5 \not\equiv 1$

$4^5 \equiv 2^{10} \equiv 1204 \equiv 1$ NO   4 di grado 5

$\begin{cases} 9^2 \equiv 81 \equiv 4 \not\equiv 1 \\ 9^5 \equiv 3^{10} \equiv \underset{048}{59049} \equiv 1 \end{cases}$ NO   9 di grado 5

$10^2 \equiv 100 \equiv 1$ NO

$\begin{cases} 6^2 \equiv 36 \equiv 3 \not\equiv 1 \\ 6^5 \equiv \underset{66}{7776} \equiv 10 \not\equiv 1 \end{cases}$ OK

$6^{10} \equiv 1$ OK

$8^2 = 64 \equiv 9 \not\equiv 1$

$8^5 = 2^{15} \equiv 327\underset{58}{68} \equiv 10 \not\equiv 1$ OK

$8^{10} \equiv 1$ OK

$2^{30} \equiv 107374\overset{823}{1824} \equiv 1$ OK

$97612893 \times 11 =$

1 è di ordine 1 (n>0) minimo

Residui quadratici

p primo > 2, dispari

$$a \in \mathbb{Z}_p^* \qquad a \perp p$$

quali $\quad a \equiv b^2 \pmod p$?

$a = \{1, 2, \dots (p-1)\}$, $(p-1)$ residui in $\mathbb{Z}_p^*$

$\varphi(p) = p-1$

radici primitive $= \varphi(p-1)$ ($p-1$ pari comunque)

quali a sono **residui quadratici** tali che

$$a = b^2$$

e cioè a ha due radici $\pm b$ esattamente

Per calcolare i quadrati in $\mathbb{Z}_p^*$ basta prendere

$$b = 1, 2, 3 \dots \frac{(p-1)}{2}$$

e fare $\quad b^2 \bmod p$

per i rimanenti

$$+\frac{(p-1)}{2}+1, \frac{(p-1)}{2}+2 \dots (p-1)$$

risultano tutti $\equiv -b \pmod p$ per alcuni b.

Per la precisione sono metà degli elementi di $\mathbb{Z}_p^*$, nel senso di $\left(\frac{p-1}{2}\right)$, che sono quadrati.

ES. $p=11$ $\qquad \mathbb{Z}_{11}^* = \{1,2,3,4,5,6,7,8,9,10)$

$(p-1) = 10$ elementi

$\frac{p-1}{2} = 5$ elementi
sono quadrati
e sono <u>residui quadratici</u>

gli altri
$\frac{p-1}{2} = 5$ elementi sono <u>non residui</u>

i residui sono:

b	
1	$1^2 = 1$
2	$2^2 = 4$
3	$3^2 = 9$
4	$4^2 = 16 = 5$
5	$5^2 = 25 = 3$

$a_q = 1, 3, 4, 5, 9$

i non residui sono:

$-b$

$(-5)^2 = 6^2 \equiv 36 \equiv 3$

$(-4)^2 = 7^2 \equiv 49 \equiv 5$

$(-3)^2 = 8^2 \equiv 64 \equiv 9$

$(-2)^2 \equiv 9^2 \equiv 81 \equiv 4$

$(-1)^2 \equiv 10^2 \equiv 100 \equiv 1$

$a_{\bar{q}} = 2, 6, 7, 8, 10$

non c'è $b^2 \equiv a_{\bar{q}} \pmod{p}$

Se $\alpha = g$ è un elemento generatore di $\mathbb{Z}_p$ (3)

Allora $g^{i} = \left(\pm g^{\frac{i}{2}}\right)^2 = a_q = g^{i}$ con i pari

$a_{\bar{q}} \equiv g^{i}$ con i dispari

ES. $p = 11$ $\quad p-1 = 10 = 2 \times 5$ $\quad$ es. $g = 2$

$g^{\frac{10}{2}} \equiv g^5 \equiv 2^5 = 32 = 10 \not\equiv 1$ OK

$g^{\frac{10}{5}} \equiv g^2 \not\equiv 1$ $\quad 2^2 = 4 \not\equiv 1$ OK

$g = 2$

$2^0 \equiv 1$

$a_q = g^{i\,\text{PARI}}$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 \equiv 16 \equiv 5$

$2^5 \equiv 32 \equiv 10$

p $\quad 2^6 \equiv 64 \equiv 9$

$2^7 \equiv 128 \equiv 7$

(mod 11)

$2^8 \equiv 256 \equiv 3$

$p-2$ $\quad 2^9 \equiv 512 \equiv 6$

$p-1$ $\quad 2^{10} \equiv 1024 \equiv 1$

$p=11 \qquad p-1=10=2\times 5$

$\alpha=3 \qquad 3^5\equiv 243\equiv 1$ NO $\qquad$ mod 11

$3^2\equiv 9\not\equiv 1$ OK

$\alpha=4 \qquad 4^5\equiv 2^{10}\equiv 1024\equiv 1$ NO

$\alpha=5 \qquad 5^5\equiv 15625\equiv 1$ NO

$\alpha=2 \qquad \left.\begin{array}{l} 2^5\equiv 32\equiv 10\not\equiv 1 \\ 2^2\equiv 4 \quad \not\equiv 1 \end{array}\right\}$ OK $\quad 2$

$\alpha=6 \qquad \left.\begin{array}{l} 6^5\equiv 10\not\equiv 1 \\ 6^2\equiv 36\equiv 4\not\equiv 1 \end{array}\right\}$ OK $\quad 6$

Let

$\underline{\alpha=g=2}$

	a_g		$b=2^{\frac{j}{2}}$
	$2^2\equiv 4$	$j=2$	$2^{\frac{2}{2}}=2$
	$2^4\equiv 5$	$j=4$	$2^2=4$
	$2^6\equiv 9$	$j=6$	$2^3=8$
	$2^8\equiv 3$	$j=8$	$2^4=16\equiv 5$
	$2^{10}\equiv 1$	$j=10$	$2^5\equiv 32\equiv 10$

$b=\pm 2, \pm 4, \pm 8, \pm 5, \pm 10.$

$b^2\equiv a \pmod p$

$\underline{a=4,5,9,3,1}$

$$x^2 \equiv a \pmod{p}$$

Esempio $p = 13$ $\qquad p \equiv 1 \pmod{4}$

Trovare i residui quadratici di $\mathbb{Z}_p^*$, $a \in \mathbb{Z}_p^*$

$\mathbb{Z}_p^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ RQ $\qquad p-1 = 12 = 3 \times 2^2$

6 quadratici $\qquad \frac{p-1}{2} = 6$

6 non residui

Trovo un elemento primitivo es. 2

$$\begin{cases} 2^{\frac{12}{3}} \equiv 2^4 \equiv 16 \equiv 3 \pmod{13} \neq 1 & \text{ok} \\ 2^{\frac{12}{2}} \equiv 2^6 \equiv 64 \equiv 12 \pmod{13} \neq 1 \end{cases}$$

$2^1 \equiv 2 \equiv 2$

$2^2 \equiv 4 \equiv 4 \to x = 2 \to 2^2 = 4$ $\qquad \pm 2$

$2^3 \equiv 8 \equiv 8$

$2^4 \equiv 16 \equiv 3 \to x = 4 \to 4^2 \equiv 16 \equiv 3$ $\qquad \pm 4$

$2^5 \equiv 32 \equiv 6$

$2^6 \equiv 64 \equiv 12 \to x = 8 \xrightarrow{(\mathrm{mod}\ 13)} 8^2 \equiv 64 \equiv 12$ $\qquad \pm 8$

$2^7 \equiv 128 \equiv 11$

$2^8 \equiv 256 \equiv 9 \to x = 3 \to 3^2 \equiv 9$ $\qquad \pm 3$

$2^9 \equiv 512 \equiv 5$

$2^{10} \equiv 1024 \equiv 10 \to x = 6 \qquad 6^2 \equiv 36 \equiv 10$ $\qquad \pm 6$

$2^{11} \equiv 2048 \equiv 7$

$2^{12} \equiv 4096 \equiv 1 \to x = 1 \qquad 1^2 \equiv 1$ $\qquad \pm 1$

Congruenze

ESEMPIO

$E_K(P)=C$

CIFRARIO AFFINE

$$\underset{\text{plaintex}}{P} \longrightarrow \boxed{CA} \longrightarrow \underset{\text{ciphertext}}{C}$$

$$\uparrow K$$

$C, P \in \mathbb{Z}_m$

- $C \equiv (aP+b) \pmod m$

per due interi a, b ; sia $b \in \mathbb{Z}_m$

e che sia poi

- $P \equiv a^{-1}(C-b) \pmod m$

per cui a^{-1} esiste se $a \in \mathbb{Z}_m^*$

e cioè se $\mathrm{mcd}(a,m)=1$.

la chiave è $(a,b) \equiv K$

ove $b \in \mathbb{Z}_m$ e $a \in \mathbb{Z}_m^*$

$|K| = |a| \cdot |b| = \varphi(m) \cdot m = m\varphi(m)$

key space $= m\varphi(m)$

Prendiamo l'alfabeto italiano $m=21$

$m = 3 \cdot 7 = 21 = p \cdot q$

$\begin{cases} A\ B\ C\ D\ E \cdots\ S\ T\ U\ V\ Z \\ 0\ 1\ 2\ 3\ 4 \ldots\ 16\ 17\ 18\ 19\ 20 \end{cases}$

qual'è il cifrario affine, e cioè per quale chiave $K \equiv (a, b)$ il testo d'ingresso $P_1, P_2 \equiv SI$ viene cifrato in $C_1 C_2 \equiv NO$

$P_1 = 16 \to C_1 = 11$

$P_2 = 8 \to C_2 = 12$

Risolviamo un sistema di congruenze a due incognite a e b

$$\begin{cases} [1] \quad 11 \equiv a\,16 + b \pmod{21} \\ [2] \quad 12 \equiv a\,8 + b \pmod{21} \end{cases}$$

moltiplico la [2] per 2 e sottraggo la [1]

$$13 \equiv b \pmod{21}$$

e poi sostituisco nella [2]

$$a\,8 + 13 \equiv 12 \pmod{21}$$

$$a\,8 \equiv -1 \equiv 20$$

per cui $\qquad a \equiv 8^{-1} \cdot 20 \qquad\qquad \varphi(21) = 2 \cdot 6 = 12$

$\mathrm{mcd}(8, 21) = 1$ ok!

$$8^{-1} \equiv 8^{\varphi(21)-1} \equiv 8^{11} \equiv 8 \pmod{21}$$

infatti

	1
1	$1^2 \cdot 8 \equiv 8$
0	$8^2 \equiv 64 \equiv 1$
1	$1^2 \cdot 8 \equiv 8$
1	$8^2 \cdot 8 \equiv \underline{8}$

mod 21

allora $\quad a \equiv 8 \cdot 20 \equiv 13 \pmod{21}$

allora $\quad E_K(P) \equiv 13P + 13 \pmod{21}$

<u>cipher</u>

<u>decipher</u>

$a \equiv 13 \qquad \mathrm{mcd}(13, 21) = 1$

$$a^{-1} \equiv 13^{-1} \equiv 13^{11} \equiv 13 \pmod{21}$$

	1
1	$1^2 \cdot 13 \equiv 13$
0	$13^2 \equiv 169 \equiv 1$
1	$1^2 \cdot 13 \equiv 13$
1	$169 \cdot 13 \equiv 2197 \equiv \underline{13}$

Potenze

$a^4 \bmod n \qquad 3^4 \bmod 2$

$(a \cdot a \cdot a \cdot a) \bmod n$

$81 \bmod 2 = 1$

oppure

$3^4 \bmod 2 \quad (3 \bmod 2)^4 \bmod 2 \equiv (1)^4 \equiv 1 \pmod 2$

$8^{11} \bmod 21 \equiv (8^5 \cdot 8^5 \cdot 8) \bmod 21 =$

$\left[(8^5 \bmod 21)^2 \cdot 8\right] \bmod 21$

$\left[(2^{15} \bmod 21)^2 \cdot 8\right] = \left[(32.768 \bmod 21)^2 \cdot 8\right]$

$= \left[32.768 - \left\lfloor \frac{32.768}{21} \right\rfloor \cdot 21\right]^2 \cdot 8 \bmod 21$

$= \quad 8^2 \cdot 8 = 2^9 \bmod 21 = 512 \bmod 21 =$

$= 8$

$X = P \,;\; Y = C$

$$y = E_k(x) = (ax+b) \bmod m$$

$m = 16 = 2^4$

$$\begin{cases} a = 13 \\ b = 15 \end{cases} \qquad \text{mcd}(a,m) = 1 \quad \text{ok}$$

$$x = a^{-1}(y-b) \bmod m = D_k(y)$$

$\varphi(m) = 2^4 - 2^3 = 8 \qquad a^{-1} \equiv a^7 \equiv 13^7 \equiv 5 \pmod{16}$

$13^7 \bmod 16 = 5$

	1
1	$1^2 \cdot 13 \equiv 13$
1	$13^2 \cdot 13 \equiv 2197 \equiv 5$
1	$5^2 \cdot 13 \equiv 325 \equiv 5$

infatti

$$5 \cdot 13 \equiv 65 \equiv 1 \pmod{16}$$

$\bar{a}^{1} \bmod 16$ $\qquad a = 13 \quad m = 16$ $\qquad \underline{13 \bmod 16}$

$m > a$

passo	q_i	t	s
		$t_0 = 0$	$s_0 = 1$
	r_2	$t_1 = 1$	$s_1 = 0$
1	$16 = 1 \cdot 13 + 3$	$t_2 = -1$	$s_2 = 1$
$n-1$ 2	$13 = 4 \cdot 3 + 1^{r_3}$	$t_3 = 1+4=5$	$s_3 = -4$
$n=3$	$3 = 3 \cdot 1 + 0$	$-1-15= -16$	$1+12 = 13$
			OK

$\bar{a}^{1} \equiv 5 \equiv t_n = t_3$ $\bmod 16$

$\mathrm{mcd}(13,16) = 1 = r_n = r_3$

$t_{n+1} = t_4 = (-1)^n \cdot 16 = -16 = -m$

$s_{n+1} = s_4 = (-1)^{n+1} 13 = 13 = a$

$$5 \cdot 13 - (4 \cdot 16) = 65 - 64 = 1 \pmod{16}$$

$$\Delta = t_n \cdot s_{n+1} - s_n \cdot t_{n+1} = (-1)^{n+1} = 1$$

vale anche che

$$s_n \cdot m + t_n a = 1 = r_n$$

$$(-4) \cdot 16 + 5 \cdot 13 = 1 \pmod{16}$$

ma anche

$$s_{n-1} m + t_{n-1} a = r_{n-1}$$

$$s_2 \cdot 16 + t_2 13 = r_2$$

$$1 \cdot 16 + -1 \cdot 13 = 3$$

ok

$$\det \begin{bmatrix} t_n & s_n \\ t_{n+1} & s_{n+1} \end{bmatrix} = t_n s_{n+1} - s_n t_{n+1} = (-1)^{n+1}$$

n passi AEE

congruenza $ax \equiv b \pmod{m}$

esempio
$m = 26 = 2 \cdot 13$
$\varphi(m) = 12$

$x \equiv a^{-1} \cdot b \pmod{m}$
se $mcd(a, m) = 1$

$ax \equiv b \pmod{m}$

se $mcd(a, m) = d > 1$
e se $d \mid b$
allora ha soluzione
se $d \nmid b$ NON ha soluzione

esempio $2x \equiv 1 \pmod{6}$
$mcd(2, 6) = d = 2$
ma $d \nmid b$ $2 \nmid 1$
NON HA SOLUZIONE

Se invece

(1) $15x \equiv 6 \pmod{21}$

allora $mcd(15, 21) = d = 3$

e $d \equiv 3 \mid 6$

ci sono $d = 3$ soluzioni

la soluzione x_0 della congruenza derivata da (1)

$$\frac{15}{d} x_0 \equiv \frac{6}{d} \left(\mod \frac{21}{d}\right)$$

per $d = 3$

$$5x_0 \equiv 2 \pmod 7$$

allora $x_0 \equiv 5^{-1} \cdot 2 \pmod 7$

$\exists 5^{-1}$: $mcd(5, 7) = 1$

$5^{-1} \mod 7 \equiv 5^5 \mod 7 \equiv 3$

$p = 7 \rightarrow p - 2 = 5$

$x_0 \equiv 6 \mod 7$

SOLUZIONI $\{6; 13; 20\}$

e le altre due soluzioni sono

$13 = x_1 = x_0 + 1 \cdot \frac{m}{d} = 6 + 7 = 13$ mod 21

$20 = x_2 = x_0 + 2 \cdot \frac{m}{d} = 6 + 14 = 20$ mod 21 se

$m > a$

$$s \cdot m + t a = 1$$

$mcd(m,a)=1$

poniamo ora che

$m = p$ e $a = q$ primi $p > q$

quindi $mcd(p,q)=1$

e che sia $n = p \cdot q$

allora posso scrivere che se

$$X \equiv b \pmod{n}$$

allora $\begin{cases} X \equiv b_1 \bmod p \\ X \equiv b_2 \bmod q \end{cases}$

es. se $X \equiv 26 \pmod{35}$ $p = 7$ $q = 5$ $n = 35$

allora

$\begin{cases} X \equiv 26 \equiv 5 \bmod 7 \\ X \equiv 26 \equiv 1 \bmod 5 \end{cases}$ $b_1 = 5$ $b_2 = 1$

vale allora che

$$X \bmod n = b_2 s p + b_1 t q$$

nel caso $p=7$ e $q=5$ si ha

	0	1
	1	0
$7 = 1 \cdot 5 + 2$	-1	1
$5 = 2 \cdot 2 + 1$	3	-2
$2 = 2 \cdot 1 + 0$	-7	5

$t = 3 \quad s = -2$

allora $X \bmod 35 = 1 \cdot (-2) \cdot 7 + 5 \cdot 3 \cdot 5 =$
$= -14 + 75 = 61 = 26$

$X \equiv 26 \bmod 35$

$m > a$ si ha che $t_{max} = a^{-1} \bmod m$ e $s_{max} = m^{-1} \bmod a$

se $\mathrm{mcd}(m, a) = 1$

- $t_{max} = 3 = 5^{-1} \bmod 7$
- $s_{max} = -2 = 3 = 7^{-1} = 2^{-1} \bmod 5$

$s_{max} = -2 = 3 \bmod 5 = (7 \bmod 5)^{-1} \bmod 5 = 2^{-1} \bmod 5$