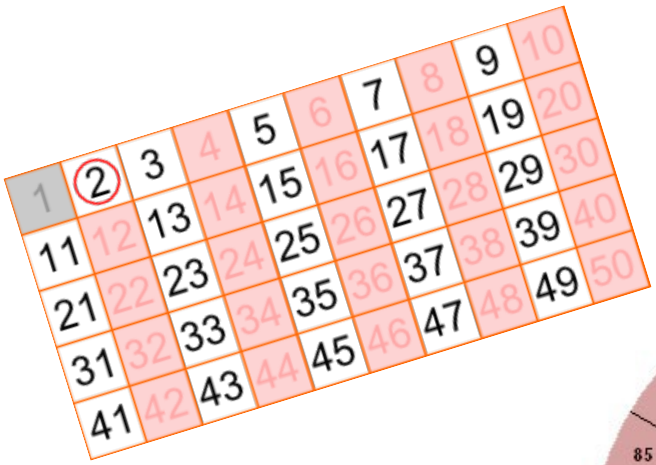
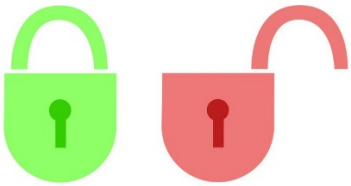
Istituto Statale 'Biagio Pascal'
Istituto Tecnico Tecnologico – Liceo Scientifico
Via Brembio,97- 00188 - Via dei Robilant,2 - 00194 – Roma
Centralino: 06-12112-4205 via Brembio - 06-12112-4225 Via dei Robilant
Codice meccanografico RMTF330002 C.F. 97046890584 Web: www.itispascal.it
Email: RMTF330002@istruzione.it Pec: RMTF330002@pec.istruzione.it

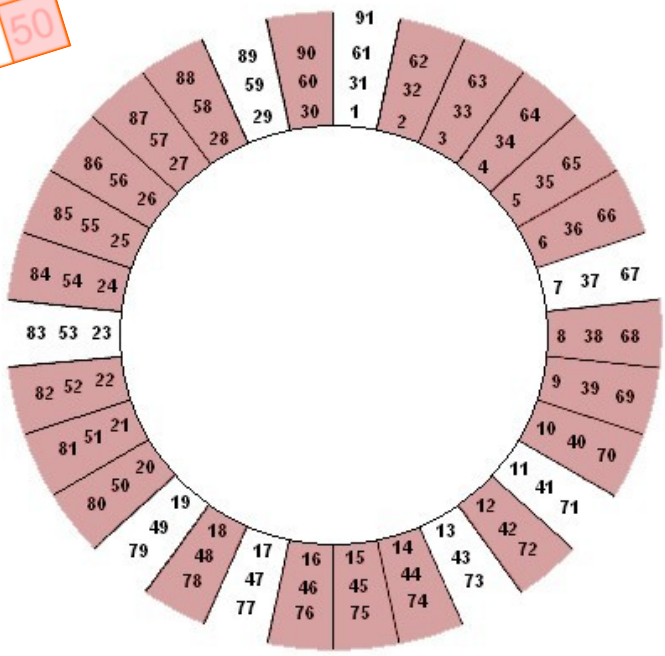
Liceo Matematico

U.D. 5

Numeri primi, crivelli e crittografia







Obiettivi formativi

Correttezza nel ragionamento

Obiettivi didattici
- Saper definire in maniera corretta i numeri primi
- Saper dimostrare il teorema sull'infinità dei numeri primi (Euclide)
- Ricercare i numeri primi – crivello di Eratostene

Prerequisiti
- Operazioni con i numeri naturali

Materiale

- Schede di esercitazione e verifica

Esperienza
1. Definizione di numeri primi
2. Perché il numero 1 non è primo?
3. Quanti sono i numeri primi?
4. Come stabilire se n è primo? Crivello di Eratostene. **Scheda n° 1 – numeri primi da 2 a 100.**
5. Metodo della ruota di fattorizzazione (Wheel Factorization**)**
6. Crittografia – cenni al metodo R.S.A

Verifica
1. **Scheda n° 1 – numeri primi da 2 a 100.**
2. **Attività:** esempio di crittografia a chiave pubblica con scatole e lucchetti

Tempi: 2 ore

1. **Definizioni di numeri primi:**

un numero primo p: è un numero naturale maggiore di 1 che ammette solo 2 divisori: 1 e il numero stesso.

Anche:

un intero positivo n si dice primo se ha esattamente due divisori positivi.

Questa definizione di numero primo è diversa da quella che la maggior parte delle persone ricorda dalle Scuole Medie: "un intero positivo n si dice primo se è divisibile solo per 1 e per se stesso". Il motivo principale per cui diamo questa definizione è che vogliamo **escludere il numero 1 dall'insieme dei numeri primi.**

Per questo motivo, gli interi n = 2 che non sono numeri primi si dicono composti.

2. **Perché il numero 1 non è primo?**

Ricordiamo il **teorema fondamentale dell'aritmetica**.

Ogni numero naturale diverso da 0 e da 1 o è primo, o è il prodotto di fattori primi. Tale decomposizione in fattori primi è unica a meno dell'ordine dei fattori.

Se 1 fosse primo non varrebbe l'unicità, cioè potremmo pensare a $6 = 2*3$ oppure a $6 = 2 * 3 *1$

3. **Quanti sono i numeri primi?**

Teorema: esistono infiniti numeri primi (dimostrazione di Euclide 300 a.c.)

Dimostrazione:
Supponiamo (per assurdo) che l'insieme dei numeri primi sia finito $P = \{p_1, p_2, p_3, \ldots, p_t\}$.
Il numero $n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_t + 1$ che si ottiene calcolando il loro prodotto e aggiungendo 1 è tale che o

- n non è un numero primo, ma allora ammette un divisore primo che **non compare tra gli** $p_k \in P$, in quanto il resto della divisione di n per ciascun p_k è uguale a 1

oppure

- n è un numero primo maggiore di p_t e quest'ultimo dunque **non era il più grande** di tutti i primi.
- In ogni caso giungiamo ad una contraddizione. Dunque la premessa, l'insieme dei numeri primi è finito, è falsa.

4. **Come stabilire se n è primo? Crivello di Eratostene.**

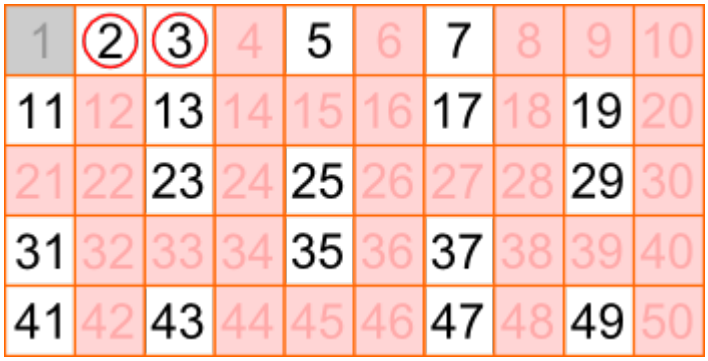
E' un metodo risalente ad Eratostene (Cirene, 276 a.C. circa – Alessandria d'Egitto, 194 a.C.) che permette di trovare tutti i numeri primi minori o uguali di un numero fissato.
Vediamo come determinare tutti i numeri primi minori di 50.
Costruiamo una tabella come in figura.
Cancelliamo l'uno perché non è primo.
Cerchiamo il due e cancelliamo tutti i multipli di due

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Cancelliamo l'uno perché non è primo.
Cerchiamo il due e cancelliamo tutti i multipli di due

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Ora cerchiamo il tre e cancelliamo tutti i multipli di tre



Nello stesso modo procediamo con 5,7,11,13,17,19,23,29,31,37,41,43,47

I numeri cerchiati sono primi.

SCHEDA N° 1 – CRIVELLO DI ERATOSTENE

Utilizzando il Crivello di Eratostene individuare i numeri primi fino a 100.

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	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

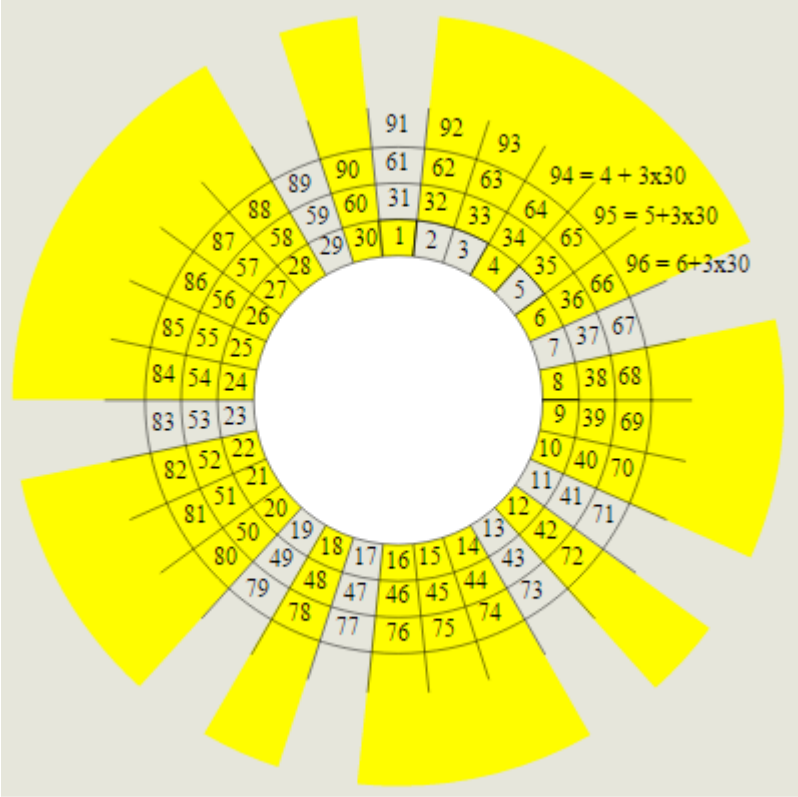
Trascrivili qui:

5. Metodo della ruota di fattorizzazione (Wheel Factorization)

Il metodo della ruota risulta più efficiente del crivello di Eratostene

Si scelgono inizialmente come numeri primi di partenza: 2, 3, 5 per ottenere una **ruota di lunghezza 30**.

La lunghezza della ruota è determinata dal prodotto dei numeri primi che decidiamo di utilizzare. Nel nostro caso 2 * 3 * 5 = 30.



Passo 1) cancelliamo (con il giallo) il numero 1 perché non è primo

Passo 2) cancelliamo nel primo "giro" tutti i multipli di 2, di 3 e di 5

Passo 3) cancello tutti i numeri k congrui a un numero non primo h del primo giro cioè divisibile per 2, 3, o 5 supponiamo divisibile per 3

allora k = h + t30 ma h è divisibile per 3 (h=3f) quindi

k= 3f +t30 = 3(f+t10) allora k non è primo

«Quindi i possibili numeri primi possono trovarsi solo nelle zone non colorate di giallo nella figura».

6. Crittografia

Con il termine *crittografia* (abbiamo visto nella precedente u.d.) intendiamo lo *studio dei metodi che consentono la trasmissione sicura dell'informazione.*

Usualmente si distingue tra due diversi tipi di crittografia:

a) ***a chiave segreta***: è il metodo classico (usato già dagli antichi romani) ed è utile solamente nel caso vi siano pochi utenti poiché è necessario che ogni utente preventivamente concordi e scambi la propria chiave segreta con un altro utente;
b) ***a chiave pubblica***: è il metodo moderno e consente una trasmissione sicura anche nel caso di molti utenti poiché non necessita di uno scambio preventivo delle chiavi segrete. E' stato proposto per la prima volta da Diffie e Hellman nel 1976.

A prima vista la crittografia a chiave pubblica sembra impossibile.

Per convincersi del contrario proponiamo l'esempio classico del doppio *lucchetto.*

Supponiamo di avere due utenti A e B e che A voglia spedire un messaggio segreto a B

1. A mette il messaggio in una scatola che chiude con il suo lucchetto L_A (di cui lui solo ha la chiave e che spedisce a B
2. B riceve la scatola chiusa con L_A, aggiunge il suo lucchetto L_B (di cui lui solo ha la chiave) e rispedisce il tutto ad A
3. A, ricevuta la scatola con il doppio lucchetto, toglie il lucchetto L_A e rispedisce la scatola a B
4. A questo punto, ricevuta la scatola, B può togliere il lucchetto L_B e leggere il messaggio di A

La sicurezza di questo schema risiede nel fatto che le chiavi per aprire i due lucchetti sono conosciute solamente dai rispettivi proprietari, che non le hanno preventivamente concordate e scambiate.

Una delle "versioni matematiche" di tale idea è il metodo crittografico e a chiave pubblica R.S.A., propost da Rivest, Shamir ed Adleman nel 1978.

In poche parole:

per **codificare il messaggio** bisogna saper costruire numeri primi grandi, tale operazione è computazionalmente *veloce*;

per **violare il sistema** bisogna saper fattorizzare interi grandi ottenuti come prodotto di due primi, tale operazione è computazionalmente *lenta*;

Tale marcata differenza tra la velocità di esecuzione delle operazioni di costruzione di numeri primi grandi e di fattorizzazione di interi grandi garantisce la sicurezza del metodo, almeno per un tempo sufficientemente lungo.

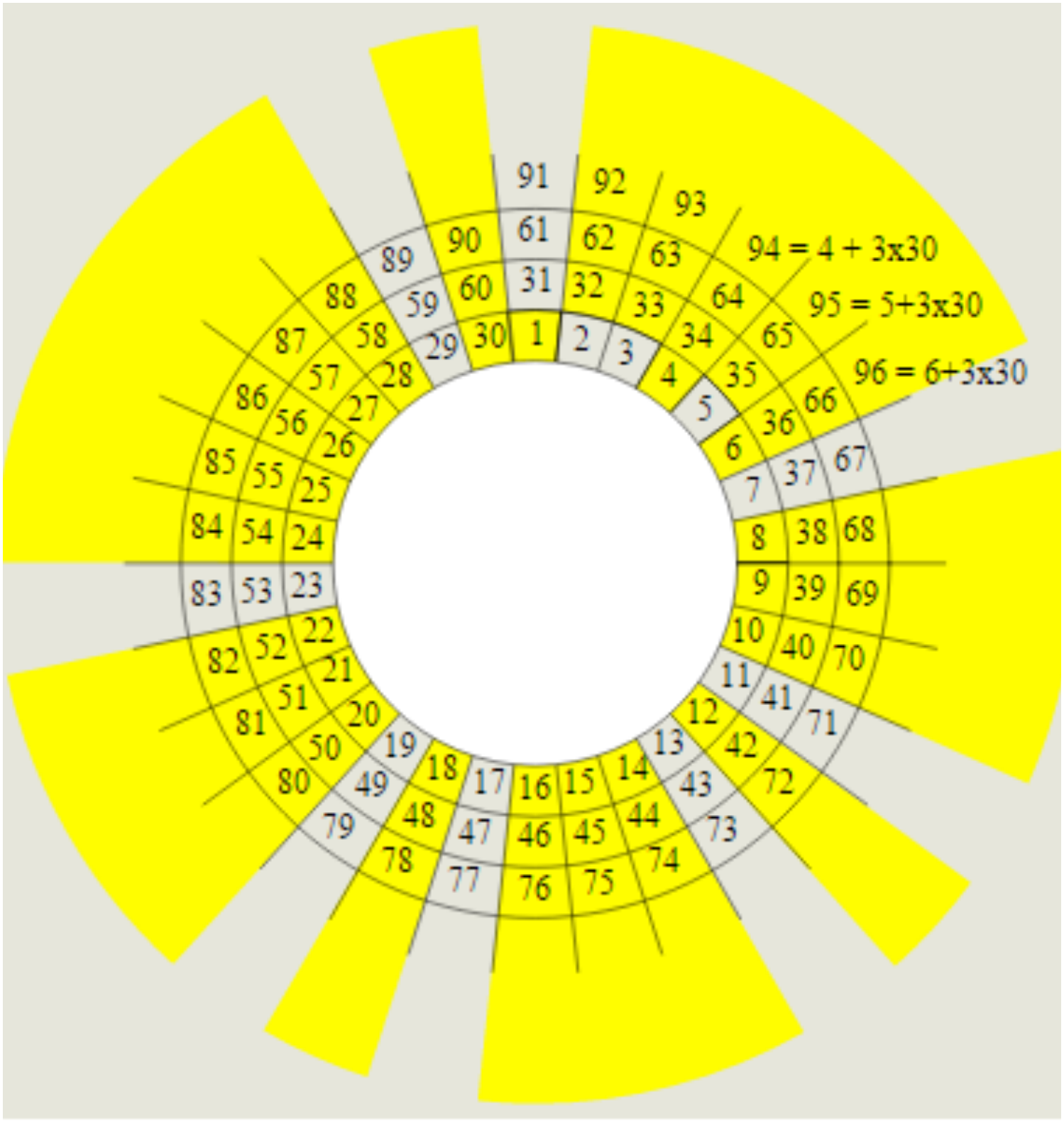
Ad esempio, con la tecnologia attuale, per calcolare il prodotto di due primi casuali bastano pochi secondi su un computer disponibile in commercio mentre l'operazione di fattorizzazione di un intero di 140 cifre in base 10 richiede, utilizzando vari supercomputers operanti parallelamente circa un mese!

Incrementando il numero di cifre si aumenta la sicurezza del sistema: attualmente si raccomanda di utilizzare interi con almeno 220 cifre in base 10

Attività

Preparare alcune scatole e un lucchetto con chiave per ogni gruppo di lavoro.

Mettere in pratica il metodo dei lucchetti per il passaggio di messaggi segreti con chiave pubblica


91
92
93
94 = 4 + 3x30
95 = 5+3x30
96 = 6+3x30
90
89
88
87
86
85
84
83
82
81
80
79
78
77
76
75
74
73
72
71
70
69
68
67
66
65
64
63
62
61
60
59
58
57
56
55
54
53
52
51
50
49
48
47
46
45
44
43
42
41
40
39
38
37
36
35
34
33
32
31
30
29
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