Da un'idea di Katia Silvia Arensi
Sara Belfanti
Chiara Colombo
Beniamino Lanteri
Corsisti SILSIS classe A059

A spasso con i numeri primi

Scopo dell'attività

L'attività è pensata per arricchire la presentazione di un argomento cosi importante come quello dei numeri primi, dando uno stimolo in più agli studenti e sottolineando in particolare l'importanza dei numeri primi nella crittografia.

Materiali

- Fogli di carta bianchi, matite, pastelli o pennarelli, cartine delle regioni italiane
  - Orologio
  - Calcolatrice

Attività

- L'insegnante comincerà a spiegare l'origine semantica della parola ***crittografia*** e ad accennare ai contenuti e alle metodologie proprie di questa disciplina, quindi inviterà i Probabilmente gli alunni proporranno esempi quali la password del computer, il codice segreto del bancomat o il PIN del cellulare; sfruttando le indicazioni e le idee scaturite dalla classe e regolando i diversi interventi il docente potrà così introdurre l'origine e l'utilizzo dei codici segreti, sottolineando l'importanza che tali codici hanno sempre avuto durante le guerre e che oggi hanno anche per proteggere informazioni di diverso tipo: dalle formule commerciali (per esempio, quella che dà conto degli ingredienti della Coca Cola), alle previsioni finanziarie o alle informazioni militari. E magari potrà accennare anche al problema degli *hackers*!

- L'insegnante introdurrà quindi alla classe i metodi crittografici più semplici, come il **CODICE DI CESARE** e il **CODICE ATBASH**.

  Per quanto riguarda il primo dei due codici, il suo nome deriva da quanto è stato scritto da Svetonio nella *Vita dei dodici Cesari*. Secondo questo storico infatti Giulio Cesare usava, per le sue corrispondenze riservate, un codice di sostituzione delle lettere dell'alfabeto molto semplice, nel quale la lettera della parola da trasmettere veniva sostituita dalla lettera che la segue di tre posti nell'alfabeto: la lettera A era

sostituita dalla D, la B dalla E e così via, fino alle ultime lettere che venivano cifrate con le prime, come nello schema che segue (che fa riferimento all'odierno alfabeto internazionale).

Chiaro	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cifrato	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Prendendo allora come esempio la frase **Auguri di buon compleanno**
e codificandola secondo il codice di Cesare, si otterrà il seguente messaggio cifrato:

Chiaro	auguridibuoncompleanno
Cifrato	dxjxulglexrqfrpsohdqqr

Più in generale oggi si dice **codice di Cesare** un codice nel quale la lettera del messaggio chiaro viene spostata di un numero fisso di posti, non necessariamente tre; un esempio è il codice che, sempre secondo Svetonio, era usato da Augusto, dove la A era sostituita dalla B, la B dalla C e così via, fino all'ultima lettera che era sostituita dalla A. Poiché l'alfabeto internazionale è composto da 26 caratteri, sono possibili (sostanzialmente) 26 codici di Cesare diversi, dei quali uno (quello che comporta uno spostamento di zero posizioni) darà un cifrato uguale al messaggio chiaro iniziale.

Per quanto riguarda invece il secondo codice, esso deriva dal libro di Geremia nella Bibbia, dove si usa un semplicissimo codice monoalfabetico per cifrare la parola Babele: la prima lettera dell'alfabeto ebraico (Aleph) viene cifrata con l'ultima (Taw), la seconda (Beth) viene cifrata con la penultima (Shin) e così via. Da queste quattro lettere è derivato il nome di **Atbash** (A con T, B con SH) per questo codice.
Usando il moderno alfabeto internazionale, l'Atbash può essere riassunto con lo schema di cifratura seguente:

CHIARO	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
CIFRATO	Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

Quindi se la frase da decifrare è **Il sole brilla**
il risultato sarà: **Rohlovyirooz**

- L'insegnante dividerà quindi i ragazzi in squadre formate al massimo da cinque alunni (si può tranquillamente lasciare che i gruppi si formino spontaneamente per simpatie o preferenze degli alunni stessi, a meno che il docente non ritenga necessario intervenire nella formazione delle squadre per motivi specifici della classe) e ogni squadra sceglierà un nome e/o un simbolo di identificazione. A questo punto si comincia il gioco.

Il viaggio misterioso

L'insegnante spiegherà che con questa attività si vuole proporre un'esperienza di decodifica di messaggi cifrati attraverso sequenze numeriche, decodifica che può essere fatta utilizzando la scomposizione in fattori primi delle sequenze e la trasformazione dei messaggi numerici in parole, attraverso un particolare codice segreto. L'utilizzo dei numeri primi rende più complesso il tradizionale codice di Cesare, diminuendo considerevolmente le possibilità di intercettare e decodificare i messaggi da parte di chi non è in possesso del codice chiave.

L'insegnante darà quindi ad ogni squadra una cartina con una determinata zona dell'Italia e due *sequenze numeriche* (che corrisponderanno a due città appartenenti alla cartina assegnata a ciascuna squadra) e spiegherà che ogni sequenza non è altro che il prodotto **tra il numero che corrisponde alla parola segreta** cifrata secondo il codice misterioso e **un numero primo arbitrario**. I ragazzi dovranno quindi, per ogni sequenza, dapprima considerarla come un numero e scomporre quest'ultimo in fattori primi. Per esempio se il numero è 3110 si avrà:

3110 = 2 x 5 x 311

Poi dovranno considerare le possibili combinazioni di prodotti ottenuti moltiplicando tutti i fattori meno uno a rotazione Nel nostro esempio dovranno scrivere:

2 x 5 = 10

2 x 311 = 622

5 x 311 = 1555

Quindi dovranno trasformare ogni prodotto in "parole", sostituendo ad ogni cifra la lettera corrispondente secondo il codice scelto (per noi, il **codice del cellulare** illustrato poco sotto), fino a trovare il **prodotto numerico che corrisponde ad una parola di senso compiuto**. Così nel nostro esempio sarà:

10 = AY-AZ	622 = PDD-PDE-PDF	1555 = AMMM-AMMN
BY-BZ	PED-PEE-PEF	AMMO
CY-CZ	PFD-PFE-PFF	AMNM-AMNN
	QDD-QDE-QDF	AMNO
	QED-QEE-QEF	…
	QFD-QFE-QFF	COMM-COMN
	RDD-RDE-RDF	COMO
	RED-REE-REF	…
	RFD-RFE-RFF	
	SDD-SDE-SDF	
	SED-SEE-SEF	
	SFD-SFE-SFF	

(Potrebbe capitare che una sequenza corrisponda a più parole di senso compiuto, si deve quindi fare molta attenzione alle sequenze numeriche che verranno date alle squadre, e quindi alle relative parole da trovare. Per esempio nel nostro caso si tratta di decodificare nomi di città, quindi nel caso della sequenza **1555** la parola **CONO** – che ha la stessa sequenza numerica di **COMO** - non potrà essere accettata, sebbene abbia significato!)

Ogni squadra dovrà trovare le due città nascoste e tracciare sulla cartina il percorso che le unisce; allo scadere del tempo a disposizione, le squadre dovranno unire le loro cartine fino a ricostruire l'intera nazione. Se avranno decifrato correttamente le sequenze assegnate, sulla cartina intera comparirà un tragitto chiuso che tocca le diverse città nascoste nelle sequenze numeriche (n.b.: perché il percorso sia chiuso e senza interruzioni ogni squadra deve avere ognuna delle due sequenze numeriche in comune con un'altra squadra, come è illustrato nell'esempio qui sotto).

Il codice attraverso il quale si è passati dalle parole alle sequenze numeriche è il cosiddetto "codice del cellulare". In questo codice ogni numero da 0 a 9 corrisponde ad una lettera o a un gruppo di lettere (in modo analogo a ciò che avviene sulle tastiere dei cellulari) secondo la tabella riportata qui sotto:

A B C	D E F	G H I	J K L	M N O	P Q R S	T U V	W	X	Y Z
1	2	3	4	5	6	7	8	9	0

Osservazione 1: sarebbe molto utile dare ai ragazzi una tabella con i primi 1000 numeri primi, in modo che possano facilmente trovare i fattori di numeri anche molto grandi.

Osservazione 2: l'insegnante potrebbe cogliere l'occasione e utilizzare l'elenco per suggerire di studiare come si comporta la sequenza di numeri primi, stimolando per esempio i ragazzi con alcune domande sulla frequenza dei primi 1000 numeri primi (quanti ce ne sono fra 1 e 100? fra 101 e 200?… fra 7001 e 8000?).

UN ESEMPIO DI GIOCO

Percorso: Prima tappa: Como-Urbino

Seconda tappa : Urbino-Rieti

Terza tappa: Rieti-Gela

Quarta tappa: Gela-Ceglie

Quinta tappa: Ceglie-Alba

Sesta tappa: Alba-Rho

Settima tappa: Rho-Como

Sequenze numeriche:

La città di partenza e di arrivo è **COMO**; quindi usando il codice del cellulare si avrà:

COMO = 1555 = 5 x 311

Allora una sequenza numerica da decifrare potrebbe essere la seguente:

3110 = 2 x 5 x 311

(l'insegnante potrà scegliere quale fattore aggiungere nella scomposizione corrispondente alla città da cui si parte, con il solo accorgimento che il fattore aggiunto dovrà essere un numero primo!).

Analogamente si avranno le altre:

da **URBINO = 761355 = 3 x 3 x 5 x 7 x 2417** si potrebbe costruire

2284065 = 3 x 3 x 3 x 5 x 7 x 2417;

da **RIETI = 63273 = 3 x 7 x 23 x 131** si potrebbe costruire

316365 = 3 x 5 x 7 x 23 x 131

da **GELA = 3241 = 7 x 463** si potrebbe costruire

16205 = 5 x 7 x 463

da **CEGLIE = 123432 = 2 x 2 x 2 x 3 x 37 x 139** si potrebbe costruire

370296 = 2 x 2 x 2 x 3 x 3 x 37 x 139

da **ALBA = 1411 = 17 x 83** si potrebbe costruire

2822 = 2 x 17 x 83

da **RHO = 635 = 5 x 127** si potrebbe costruire

3175 = 5 x 5 x 127

Perciò alle squadre saranno assegnate le seguenti sequenze:

- Squadra 1: **3110** e **2284065**
- Squadra 2: **2284065** e **316365**
- Squadra 3: **316365** e **16205**
- Squadra 4: **16205** e **370296**
- Squadra 5: **370296** e **2822**
- Squadra 6: **2822** e **3175**
    - Squadra 7: **3175** e **3110**

E ora … buon divertimento!

Elenco dei primi 1000 numeri primi

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