1. Calcolare la tabella dei numeri primi $p < 200$.

Sol. :) :) :)

2. Fattorizzare come prodotto di numeri primi i seguenti numeri: 100, 10!, 101, 1001, 10001 e il coefficiente binomiale $\binom{50}{25}$.

Sol. :) :) :)

3. (Numeri di Mersenne). Per ogni numero naturale n, si definisce l'ennesimo numero di Mersenne come $M_n = 2^n - 1$.
   (a) Fattorizzare M_n per $1 \leq n \leq 12$;
   (b) Dimostrare: se M_n è primo, allora n è primo;
   (c) Far vedere che il viceversa di (b) non vale;

   (si veda http://mathworld.wolfram.com/MersenneNumber.html)

Sol. (a) $M_1 = 1$, $M_2 = 3$, $M_3 = 7$, $M_4 = 15 = 3{\cdot}5$, $M_5 = 31$, $M_6 = 63 = 3^2{\cdot}7$, $M_7 = 127$, $M_8 = 255 = 3{\cdot}5{\cdot}17$, $M_9 = 511 = 7 \cdot 73$, $M_{10} = 1023 = 3 \cdot 11 \cdot 31$, $M_{11} = 2047 = 23 \cdot 89$, $M_{12} = 4095 = 3^2 \cdot 5 \cdot 7 \cdot 13$.
(b) Ricordiamo che per ogni $h \geq 2$ il polinomio $x^h - 1$ si decompone come $(x-1)(x^{h-1} + x^{h-2} + \ldots + 1)$. Supponiamo che $n = a \cdot b$, con $a, b \geq 2$. Allora per $x = 2^a$ ed $h = b$, abbiamo che $2^{ab} - 1$ si decompone come

$$(2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \ldots + 1), \qquad (2^a - 1) \neq 1.$$

(c) :) :) :)

4. (Numeri di Fermat) Per ogni numero naturale n, si definisce l'ennesimo numero di Fermat come $F_n = 2^{2^n} + 1$;
   (a) Dimostrare: se $2^m + 1$ è primo, allora m è potenza di 2;
   (b) Far vedere che F_n è primo per $1 \leq n \leq 4$;

   (si veda http://mathworld.wolfram.com/FermatNumber.html)

Sol. (a) Ricordiamo che per ogni $h \geq 3$ dispari, il polinomio $x^h + 1$ si decompone come $(x+1)(x^{n-1} - x^{n-2} + \ldots + 1)$. Scrivendo $m = 2^k h$, con h dispari, dall'osservazione precedente segue che $h = 1$ ed $m = 2^k$ è una potenza di 2.
(b) :) :) :)

5. Siano n ed A interi positivi. Supponiamo che $\frac{A}{n}$ sia "sufficientemente piccolo" (per esempio $\frac{A}{n} \leq \frac{1}{100}$). Verificare che la percentuale di numeri primi nell'intervallo $[n - A, n + A]$ è circa $\frac{1}{\ln n}$, dove $\ln n$ indica il logaritmo in base e di n.

Sol. Sia x un intero positivo e sia $\pi(x)$ il numero di primi minori o uguali ad x (vedi Crandall-Pomerance, pag.9). La percentuale di numeri primi nell'intervallo $[n - A, n + A]$ è data da

$$\frac{1}{2A}(\pi(n+A) - \pi(n-A)) \sim \frac{1}{2A}\left(\frac{n+A}{\ln(n+A)} - \frac{n-A}{\ln(n-A)}\right). \tag{1}$$

(qui $\ln x$ indica il logaritmo naturale in base e).
Osserviamo che se $\frac{A}{n}$ è "sufficientemente piccolo" (per esempio $\frac{A}{n} \leq \frac{1}{100}$) possiamo ragionevolmente stimare

$$\ln(n+A) \sim \ln(n-A) \sim \ln n :$$

infatti

$$\ln(n \pm A) = \ln n(1 \pm \frac{A}{n}) = \ln n + \ln(1 \pm \frac{A}{n}) \sim \ln n.$$

Dunque l'espressione (1) diventa

$$\frac{1}{\ln n}\left(\frac{(n+A)-(n-A)}{2A}\right)=\frac{1}{\ln n}.$$

Osservazione. Sia $p=\frac{1}{\ln n}$ la probabilità di trovare un numero primo nell'intervallo $[n-A,n+A]$. La probabilità di trovare un numero composto dopo $k\ln n$ tentativi è data da

$$(1-\frac{1}{\ln n})^{k\ln n}.$$

Per n molto grande, $(1-\frac{1}{\ln n})^{k\ln n}$ si può approssimare con $(\frac{1}{e})^k$ e dunque diventa arbirariamente piccolo al crescere di k. Di contro, aumenta la probabilità di trovare un numero primo.
La conseguenza di ciò è la seguente:
prendendo $k\ln n$ numeri a caso e passandoli al test di Miller-Rabin abbiamo un altissima probabilità di trovare un numero primo; al tempo stesso la complessità del calcolo rimane polinomiale $\mathcal{O}(k\ln n\cdot\log^3 n)$. Dunque costruire numeri primi grandi è "fattibile".

6. Sia n un numero di 100 cifre decimali. Stimare la percentuale di numeri primi in un intervallo $[n-A,n+A]$, con A numero di 50 cifre.

Sol. In questo caso $n\sim 10^{100}$ ed $A\sim 10^{50}$, per cui $\frac{A}{n}\sim\frac{1}{10^{50}}$ è "piccolo". Dunque la percentuale di numeri primi in un intervallo $[n-A,n+A]$ è all'incirca di

$$\frac{1}{\ln 10^{100}}\sim\frac{1}{100\ln 10}=\frac{1}{230},\qquad \ln 10=2,30....$$

Osserviamo che i numeri dell'intervallo $[n-A,n+A]$ sono numeri di 100 cifre decimali, che hanno in comune almeno le prime 50. Se prendiamo un numero a caso in questo intervallo troveremo sicuramente un numero primo che differisce da esso solo nelle ultime 3 cifre.

7. Verificare che per $n=10^8$ ed $A=150000$ l'intervallo $[n,n+A]$ contiene circa 8143 numeri primi.

Sol. In questo caso $n\sim 10^8$ ed $A=150000$, per cui $\frac{A}{n}\sim\frac{15}{10000}$ è "piccolo". Dunque il numero di primi p nell'intervallo $[n,n+A]$ è all'incirca di

$$\pi(n+A)-\pi(n)\sim\frac{n+A}{\ln(n+A)}-\frac{n}{\ln(n)}\sim\frac{A}{\ln n}=\frac{150000}{8\ln 10}\sim 8143.$$

8. Siano $B=2$ e $B=3$. Chi sono i numeri 2-smooth e i numeri 3-smooth? Elencare i primi 10 numeri 2-smooth e i primi 15 numeri 3-smooth. Verificare che sono infiniti e che crescendo si diradano.

Sol. I numeri 2-smooth numeri i cui divisori primi sono minori o uguali a 2. Dunque sono le potenze di 2

$$1,\ 2,\ 4,\ 8,\ 16,\ 32,\ 64,\ 128,\ 256,\ 512,\ 1024,\ 2048,\ \dots\ \dots$$

I numeri 3-smooth sono numeri i cui divisori primi sono minori o uguali a 3. Dunque sono della forma 2^a3^b

$$1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 16,\ 18,\ 24,\ 27,\ 32,\ 36,\ 48,\ 54,\ 64,\ \dots\ \dots$$

9. Sia $B=6$. Chi sono i numeri B-smooth? Elencare i primi 15 numeri 6-smooth.

Sol. I numeri 6-smooth sono numeri i cui divisori primi sono minori o uguali a 6. Dunque sono della forma $2^a 3^b 5^c$:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 9,\ 10,\ 12,\ 15,\ 16,\ 18,\ 20,\ 24,\ 25,\ \ldots\ \ldots$$

10. Sia B un intero positivo fissato. Siano n ed A interi con $\frac{A}{n}$ "sufficientemente piccolo". Verificare che la percentuale di numeri B-smooth nell'intervallo $[n-A, n+A]$ è data approssimativamente da u^{-u}, dove u è determinato dalla condizione $n^{1/u} = B$.

Sol. Siano B ed x interi positivi fissati e sia $\phi(x, B)$ il numero di interi B-smooth minori o uguali a x (vedi Crandall-Pomerance, pag.45). Definiamo u mediante la condizione $n^{1/u} = B$, ossia $u := \frac{\log n}{\log B}$. La percentuale di numeri B-smooth nell'intervallo $[n-A, n+A]$ è data da

$$\frac{1}{2A}\left(\psi(n+A, B) - \psi(n-A, B)\right). \tag{2}$$

Osserviamo che se $\frac{A}{n}$ è "sufficientemente piccolo" possiamo prendere lo stesso u come

$$u \sim \frac{\log(n \pm A)}{\log B} \sim \frac{\log n(1 \pm \frac{A}{n})}{\log B} \sim \frac{\log n + \log(1 \pm \frac{A}{n})}{\log B} \sim \frac{\log n}{\log B}.$$

In tal modo l'espressione (2) diventa

$$\frac{1}{2A}\left(\psi(n+A, (n+A)^{1/u}) - \psi(n-A, (n-A)^{1/u})\right) \sim \frac{1}{2A}\left((n+A)u^{-u} - (n-A)u^{-u}\right) \sim \frac{1}{u^u}.$$

11. Sia $B = 1000$ e sia $A = 10^{10}$. Stimare la percentuale di interi B-smooth compresi nell'intervallo $[10^{20} - A, 10^{20} + A]$.

Sol. In questo caso $n = 10^{20}$, $A = 10^{10}$ e dunque $\frac{A}{n} = \frac{1}{10^{10}}$ è piccolo. Estraendo il logaritmo a base 10 troviamo

$$u = \frac{\log n}{\log B} = \frac{20}{3} \sim 7,$$

da cui

$$\frac{1}{u^u} \sim \frac{1}{7^7} \sim \frac{1}{823543} \sim \frac{1}{10^6}.$$

L'intervallo in questione contiene numeri di circa 20 cifre che differiscono fra loro nelle ultime 10. Preso un numero a caso in questo intervallo, fra quelli che hanno in comune con esso le prime 14 cifre, e differiscono nelle ultime 6, ce n'è almeno uno B-smooth.
Se fissiamo $B = 10000$, nello stesso intervallo troviamo una percentuale di numeri B-smooth di $\frac{1}{5^5} \sim \frac{1}{3125}$. In questo caso, preso un numero a caso nell'intervallo, fra quelli che hanno in comune con esso le prime 16 cifre, e differiscono nelle ultime 4, ce n'è almeno uno B-smooth.

12. Sia n un numero di 100 cifre decimali e sia B un numero di 10 cifre. Stimare la percentuale di interi B-smooth in un intervallo $[n-A, n+A]$, con A numero di 50 cifre.

Sol. In questo caso $n = 10^{100}$, $A = 10^{50}$ e dunque $\frac{A}{n} = \frac{1}{10^{50}}$ è piccolo. Inoltre

$$u = \frac{\log n}{\log B} = \frac{20}{3} \sim 10,$$

da cui

$$\frac{1}{u^u} \sim \frac{1}{10^{10}}.$$

L'intervallo in questione contiene numeri di circa 100 cifre che differiscono fra loro nelle ultime 50. Preso un numero a caso in questo intervallo, fra quelli che hanno in comune con esso le prime 90 cifre, e differiscono nelle ultime 10, ce n'è almeno uno B-smooth.

13. [PC, Es.1.68] Verificare che ci sono esattamente 35084 numeri 4-smooth minori di 10^{100}.

Sol. I numeri 4-smooth sono numeri i cui divisori primi sono minori o uguali a 4. Dunque sono della forma $2^a 3^b$. Dalla disuguaglianza

$$2^a 3^b < 10^{100}$$

estraendo il logaritmo troviamo

$$a \ln 2 + b \ln 3 < 100 \ln 10.$$

Per $b = 0$, troviamo $0 \leq a \leq [100 \frac{\ln 10}{\ln 2}] = [100 \cdot 3,3219 \ldots] = 332$;
per $a = 0$ troviamo $0 \leq b \leq [100 \frac{\ln 10}{\ln 3}] = [100 \cdot 2,099 \ldots] = 209$;
per $a = 1$ troviamo $0 \leq b \leq [100 \frac{\ln 5}{\ln 3}] = [100 \cdot 1,464 \ldots] = 146$;
etc...