ESERCIZI DI TEORIA DEI NUMERI

A. BERNARDI

1. Primo foglio di esercizi

Gli esercizi con una " * " sono quelli a mio avviso più difficili.

1.1. **Algoritmo probabilistico per la fattorizzazione.** Vediamo, tramite esercizi, un algoritmo probabilistico per determinare un fattore non banale di un $N \in \mathbb{N}$.

L'algoritmo il seguente:

Se N è pari non c'è nulla da fare. Altrimenti scegli in modo random un $a \in 2, \dots, N-1$. Se $(a, N) > 1$ fatto. Altrimenti calcola r l'ordine di $[a]$ $(mod\, N)$.

(1) Se r è dispari l'algoritmo fallisce.
(2) Se r è pari, calcola $h = (a^{r/2} - 1, N)$, se $h > 1$ abbiamo finito, altrimenti l'algoritmo fallisce.

Esercizio 1. Mostrare che se $b^2 \equiv 1\,(mod\, N)$ e $b \not\equiv \pm 1\,(mod\, N)$ allora $b+1, b-1$ hanno fattori non banali in comune con N.

Esercizio 2. Mostrare che se siamo nel caso (2) si ha che $a^{r/2} + 1 \equiv 0\,(mod\, N)$.

Esercizio 3. * L'algoritmo descritto sopra ha probabilità di successo almeno $1 - \frac{1}{2^{k-1}}$ dove k è il numero dei fattori primi (distinti) di N.

(Suggerimento: Serve il teorema cinese del resto e che $|(\mathbb{Z}/p^\alpha\mathbb{Z})| = p^\alpha - p^{\alpha-1}$).

1.2. **Stime di Tchebyschev.** Miglioriamo, tramite esercizi, il bound inferiore della versione delle stime di Tchebyschev vista a lezione: qui mostriamo che

$$\pi(n) \geq \frac{n}{2\log n}.$$

Esercizio 4 (Formula di Stirling)**.** * $\ln(n!) \sim n(\ln n - 1)$.

Definiamo il coefficiente multinomiale

$$\binom{n}{p_1 n, \dots, p_d n} := \frac{n!}{(p_1 n)! \cdots (p_d n)!}$$

dove $p_1 + \cdots + p_d = 1$.

Definiamo inoltre quella che in teoria dell'informazione viene chiamata *Entropia di Shannon:*

$$H(\overline{p}) := -\sum_{i=1}^{d} p_i \log(p_i).$$

Esercizio 5. Mostrare che $\log \binom{n}{p_1 n, \dots, p_d n} = nH(\overline{p}) - O(\log(n))$

Esercizio 6. Mostrare che $\frac{n}{2} \leq \log \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Esercizio 7. Mostrare che

$$\log \binom{n}{\lfloor \frac{n}{2} \rfloor} \leq \sum_{p \leq n, p\text{primo}} \left\lfloor \frac{\log n}{\log p} \right\rfloor \log p$$

Esercizio 8. Concludere che $\pi(n) \geq \frac{n}{2 \log n}$.