ESERCIZI SULLE CONGRUENZE, 2 DICEMBRE 2008

ANDREA MAFFEI

In quello che segue con numero si intende numero intero e diciamo che a divide b se il loro rapporto è un numero intero.

Prima serie di esercizi.

Esercizio 1. Determinare tutte le soluzioni intere di $x^2 + 1 = 2^y$.

Esercizio 2. Determinare tutti i primi a, b, c, d, e, f tali che

$$a^2 = b^2 + c^2 + d^2 + e^2 + f^2.$$

Esercizio 3. Sia p un numero primo, dimostrare che per ogni x intero p divide $x^p - x$.

Questa prima serie di esercizi serve ad introdurre il concetto di congruenza.

Definizione 1. Siano a, b, n numeri interi, diciamo che a è congruo a b modulo n e scriviamo

$$a \equiv b \mod n$$

se n divide $b - a$.

Alcune semplici proprietà sono le seguenti: siano a, b, a', b', m, n numeri interi con $m \neq 0$ e sia $a \equiv a' \mod n$ e $b \equiv b' \mod n$ allora:

- $a + b \equiv a' + b' \mod n$ e $a \cdot b \equiv a' \cdot b' \mod n$;
- $ma \equiv mb \mod mn$ se e solo se $a \equiv b \mod n$;
- $a \equiv b \mod mn$ implica $a \equiv b \mod n$.

Il terzo esercizio ha la seguente generalizzazione che si chiama piccolo teorema di Fermat: sia n un intero positivo e sia x un intero primo con n (ovvero $M.C.D.(x, n) = 1$). Sia inoltre $\phi(n)$ la cardinalità dei numeri compresi tra 1 e n primi con n. Allora

$$x^{\phi(n)} \equiv 1 \mod n.$$

Seconda serie di esercizi.

Esercizio 4. Descrivere tutte le soluzioni intere dei seguenti sistemi.

$$\begin{cases} x \equiv 3 & \mod 5 \\ x \equiv 2 & \mod 7 \end{cases} \qquad \begin{cases} x \equiv 3 & \mod 6 \\ x \equiv 6 & \mod 8 \end{cases}$$

Esercizio 5. Siano x e n interi primi tra loro (ovvero $M.C.D.(x, n) = 1$). Dimostrare che esiste y tale che $xy \equiv 1 \mod n$.

Esercizio 6. Sia p un numero primo. Mostrare che $(p-1)! \equiv -1 \mod p$.

Esercizio 7. Sia p un primo dispari. Mostrare che l'equazione $x^2 \equiv -1 \mod p$ ha soluzione se e solo se $p \equiv 1 \mod 4$.

Esercizio 8. Sia p un primo dispari che sia la somma di due quadrati. Mostrare che $p \equiv 1 \mod 4$.

L'esercizio **??** ha il seguente inverso: se $p \equiv 1 \mod 4$ allora p è la somma di due quadrati.

Esercizi per casa. purtroppo per casa sono rimasti gli esercizi più difficili: in bocca al lupo!

Esercizio 9. Tra tutte le coppie m, n di interi positivi con $m < n$ tali che 1978^m e 1978^n hanno le ultime tre cifre uguali nella loro scrittura decimale, determinare quelle per cui $m + n$ è minimo.

Esercizio 10. I numeri di Fermat sono i numeri della forma $2^{(2^n)}+1$. Sulla base dell'analisi dei casi $n = 1, 2, 3, 4$ Fermat congetturò che fossero tutti primi, ma Eulero mostrò che per $n = 5$ il numero di Fermat non era primo. Mostrare che $2^{2^5} + 1$ è divisibile per 641 senza utilizzare il computer. Potete invece utilizzare il fatto che $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$.

Esercizio 11. Mostrare che per $n \geqslant 2$ il minimo intero positivo m tale che $3^m \equiv 1 \mod 2^n$ è uguale a 2^{n-2}.

Per chi volesse chiarimenti o spiegazioni può contattarmi al seguente indirizzo email: `amaffei@mat.uniroma1.it`.

Suggerimenti bibliografici. Alcuni studenti mi hanno chiesto dove possono studiare un po‘ di teoria dei numeri. Un libro, molto carino, che fa qualche teorema complicato di teoria dei numeri ma che usa strumenti elementari è *"Proofs from The Book"* di Aigner e Ziegler, edito dalla Springer. Nel libro trovate anche molte altre cose interessanti. Purtroppo non mi sembra esista una traduzione in italiano, ma di solito con la matematica il problema non è la lingua.

Purtroppo, oltre questa indicazione, non sono riuscito a pensare nulla che possa essere veramente adatto per uno studente delle superiori anche molto bravo e motivato. Forse i vostri insegnanti sanno consigliarvi meglio di me. Il suggerimento migliore, o perlomeno quello che mi sembra più ragionevole , è probabilmente quello di prendere un libro di algebra per i primi anni di università, tipo il libro di M. Artin *Algebra* della Boringhieri. Malgrado il titolo molto asciutto è un libro molto bello con un sacco di cose interessanti. Però non è un libro di teoria dei numeri, diciamo che è un libro introduttivo alla teoria dei numeri con alcuni capitoli che possono considerarsi proprio di teoria dei numeri.

Vi scrivo in ogni caso i libri di teoria dei numeri che mi sembrano più indicati. Tenete presente però che che i libri di matematica più avanzati non sono fatti per "far capire", spesso sono molto asciutti e ogni passaggio spesso richiede un grande sforzo per essere compreso quindi può essere che voi prendiate uno di questi libri e proprio non vi ci raccapezziate. In caso non vi demoralizzate è normale, e chiedete al vostro insegnati o scrivetemi all'indirizzo `amaffei@mat.uniroma1.it`. In effetti la matematica è una materia che si trasmette principalmente per via orale.

- *Primes of the form* $x^2 + n\,y^2$ di D. Cox. Questo libro studia il seguente problema: fissato n quali sono i primi che si possono scrivere nella forma $x^2 + n\,y^2$. La difficoltà di questo problema varia molto a seconda dell'n scelto e la sua risoluzione richiede tecniche diverse per essere risolto. Alcune abbastanza elementari che risalgono a Fermat altre molto più complicate che risalgono al secolo scorso. Penso potreste provare a studiare il primo capitolo.
- *Cours d'Arithmétique* di J.P. Serre (lo trovate anche in inglese). Questo libro di circa 100 pagine è diviso in due parti. Semplificando la prima illustra alcuni risultati di teoria algebrica dei numeri e la seconda di teoria analitica dei numeri. Penso potreste provare a capire il primo capitolo della prima parte e con più difficoltà il primo capitolo della seconda.

In entrambi i casi potreste avere bisogno di qualche libro di appoggio di algebra o analisi o meglio di qualche spiegazione che vi può dare il vostro insegnante o che potete chiedermi per email, perché alcune notazioni, definizioni e risultati potrebbero essere dati per scontati.

Se ne cavate qualcosa complimenti e se trovate difficoltà non esitate a contattarmi.

Ciao.
Andrea