Università degli Studi Roma Tre
Anno Accademico 2008/2009
AL1 - Algebra 1
Esercitazione 10
Giovedì 11 Dicembre 2008
http://www.mat.uniroma3.it/users/pappa/CORSI/AL1_08_09/AL1.htm
domande/osservazioni: dibiagio@mat.uniroma1.it

1. Dimostrare che se $c \equiv_a b$ allora $MCD(a,b) = MCD(a,c)$.

   Sia $d := MCD(a,b)$ e $d' := MCD(a,c)$. Per ipotesi $a \mid (c-b)$ cioè $\exists h$ tale che $ah = c - b \Leftrightarrow c = ah + b$. Quindi $d \mid a, d \mid b \Rightarrow d \mid (ah+b) = c$, perciò $d \mid d'$. Viceversa: $ah = c - b \Leftrightarrow b = c - ah$. Quindi $d' \mid a, d' \mid c \Rightarrow d' \mid b$, perciò $d' \mid d$. Quindi $d = d'$.

2. Sia p primo e $k \neq 0, p$. Dimostrare che $p \mid \binom{p}{k}$. Dedurre che $(x+y)^p \equiv_p x^p + y^p$.

   Sia $a := k!(p-k)!$, $b := p!$, $c := \binom{p}{k}$. Per quanto visto a lezione $c = b/a$ è un numero intero. $b = ac$. Inoltre $p \mid b = ac$ ma, dato che $k \neq 0, p$, $p \nmid a$. Per il lemma di Euclide $p \mid c$.
   $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} \equiv_p x^p + y^p$.

3. Dimostrare che esistono infiniti numeri primi della forma $6k+5$, con $k \in \mathbb{N}$.

   A parte $2, 3$ tutti i numeri primi sono della forma $6k+5$ o $6k+1$ al variare di $k \in \mathbb{N}$. Osserviamo poi che prodotti di numeri della forma $6k+1$ sono numeri della stessa forma: $(6k+1)(6h+1) = 36hk + 6(h+k) + 1 = 6(6hk + h + k) + 1$
   Supponiamo che i numeri primi della forma $6k+5$ siano in numero finito, $p_1 = 5, p_2, \ldots, p_n$. Si consideri $a := 6p_2 \cdot \ldots \cdot p_n + 5$. Tale numero non è divisibile né per 2 né per 3 né per 5 e, per l'osservazione, non può avere tra i suoi fattori solo primi del tipo $6k+1$. Quindi $\exists\ 2 \leq i \leq n$ tale che $p_i | a$; assurdo.

4. Scrivere 1153 in base 9, 2781 in base 5 e $(103)_7$ in base 10.

   $1153 = 9 \cdot 128 + 1$
   $128 = 9 \cdot 14 + 2$
   $14 = 9 \cdot 1 + 5$
   $1 = 9 \cdot 0 + 1$
   perciò $1153 = (1521)_9$.

   $2781 = 5 \cdot 556 + 1$
   $556 = 5 \cdot 111 + 1$
   $111 = 5 \cdot 22 + 1$
   $22 = 5 \cdot 4 + 2$
   $4 = 5 \cdot 0 + 4$
   perciò $2781 = (42111)_5$.

$(103)_7 = 1 \cdot 7^2 + 0 \cdot 7 + 3 \cdot 7^0 = 49 + 3 = 52$.

5. Risolvere le seguenti equazioni congruenziali:

   (a) $7X \equiv 4 \mod 19$;

   (b) $18X \equiv 5 \mod 51$;

   (c) $18X \equiv 6 \mod 51$;

   (d) $82X \equiv 174 \mod 13$.

   (a) $X \equiv 6 \mod 19$, ovvero l'insieme delle soluzioni è $\{6 + 19h | h \in \mathbb{Z}\}$;

   (b) dato che $MCD(18, 51) = 3 \not| 5$ allora l'equazione non è risolubile;

   (c) l'equazione ha tre soluzioni modulo 51: $6, 23, 40$, ovvero l'insieme delle soluzioni è $\{6 + 17h | h \in \mathbb{Z}\}$;

   (d) l'equazione è equivalente a $4X \equiv 5 \mod 13$ che ha un'unica soluzione modulo 13: $X = 11$. L'insieme delle soluzioni quindi è $\{11 + 13h | h \in \mathbb{Z}\}$.

6. Dimostrare che $2^{10n+1} + 19$ è divisibile per 3 per ogni $n \in \mathbb{N}$.

   Lo si potrebbe dimostrare per induzione, come già visto per casi analoghi in altre esercitazioni. Avendo ora, però, nuovi strumenti è preferibile ragionare nel modo seguente: $2^{10n+1}+19 \equiv_3 2((2^2)^{5n})+1 \equiv_3 2(1^{5n})+1 \equiv_3 2 + 1 \equiv_3 0$.

7. Dimostrare che vi sono infiniti numeri composti del tipo $10^n + 3$ (con $n \in \mathbb{N}$).

   $10 \equiv 3 \mod 7$. $10^2 \equiv 2 \mod 7$. $10^3 \equiv -1 \mod 7$. $10^4 \equiv -3 \mod 7$. $10^5 \equiv -2 \mod 7$. $10^6 \equiv 1 \mod 7$. Perciò $10^{4+6h} \equiv -3 \mod 7$ per ogni $h \in \mathbb{Z}$ e quindi, per ogni $h \in \mathbb{Z}$, $10^{4+6h} + 3 \equiv 0 \mod 7$, i.e. $7 \mid 10^{4+6h} + 4$.