Università degli Studi Roma Tre
Anno Accademico 2008/2009
AL1 - Algebra 1
Esercitazione 11
Giovedì 18 Dicembre 2008
http://www.mat.uniroma3.it/users/pappa/CORSI/AL1_08_09/AL1.htm
domande/osservazioni: dibiagio@mat.uniroma1.it

1. Risolvere i seguenti sistemi di congruenze:

$$\text{(a)} \begin{cases} X \equiv 1 & \bmod 3 \\ X \equiv 2 & \bmod 5 \\ X \equiv 3 & \bmod 7 \end{cases} \qquad \text{(b)} \begin{cases} X \equiv 5 & \bmod 6 \\ X \equiv 2 & \bmod 5 \\ X \equiv 1 & \bmod 11 \end{cases}$$

$$\text{(c)} \begin{cases} X \equiv 11 & \bmod 19 \\ X \equiv 7 & \bmod 8 \\ X \equiv 10 & \bmod 6 \end{cases} \qquad \text{(d)} \begin{cases} X \equiv 3 & \bmod 5 \\ X \equiv 1 & \bmod 63 \\ X \equiv 19 & \bmod 54 \end{cases}$$

   (a) $X \equiv 52 \mod 105$;
   (b) $X \equiv 287 \mod 330$;
   (c) il sistema non è risolubile: se $x \in \mathbb{Z}$ fosse una soluzione allora $2 \mid (x-10)$ e $2 \mid (x-7)$, quindi x sarebbe contemporaneamente pari e dispari; assurdo.
   (d) $X \equiv 883 \mod 1890$.

2. Trovare il resto della divisione di 473^{38} per 5.

   $473^{38} \equiv 3^{38} \mod 5$. Per il piccolo teorema di Fermat $3^4 \equiv 1 \mod 5$, quindi $3^{38} = 3^{4 \cdot 9} 3^2 \equiv_5 3^2 \equiv_5 4$.

3. Dimostrare che $n^7 - n$ è divisibile per 42 per ogni $n \in \mathbb{N}$.

   Per il piccolo teorema di Fermat $n^7 \equiv_7 n$. Inoltre, sempre per il piccolo teorema di Fermat, $n^2 \equiv_2 n$ e $n^3 \equiv_3 n$ quindi $n^7 \equiv_2 n$ e $n^7 \equiv_3 n$, perciò $n^7 \equiv n \mod 42$.

4. Dimostrare che per ogni primo dispari p si ha $1^p + 2^p + 3^p + \dots (p-1)^p \equiv 0 \mod p$.

   Per il piccolo teorema di Fermat sappiamo che per ogni $a \in \mathbb{Z}$, $a^p \equiv a \mod p$, quindi $1^p + 2^p + 3^p + \dots (p-1)^p \equiv 1 + 2 + \dots (p-1) \mod p$. Ma $1 + 2 + \dots + (p-1) = p\frac{p-1}{2} \equiv 0 \mod p$ e quindi la tesi è dimostrata.

5. Siano p, q numeri primi distinti. Dimostrare che $p^{q-1} + q^{p-1} \equiv 1 \mod pq$.

   Sia $x := p^{q-1} + q^{p-1}$. Per il piccolo teorema di Fermat, dato che p, q sono primi distinti, si ha che $x \equiv 1 \mod p$ e $x \equiv 1 \mod q$. Perciò $x \equiv 1 \mod pq$.

6. Dire quanti elementi ha il gruppo $(U(\mathbb{Z}_{1200}), \cdot)$.

   Il gruppo degli invertibili di $\mathbb{Z}_{1200}$ ha $\phi(1200)$ elementi. Dato che $1200 = 2^4 \cdot 3 \cdot 5^2$, allora $\phi(1200) = \phi(2^4)\phi(3)\phi(5^2) = (2^4 - 2^3) \cdot 2 \cdot (5^2 - 5) = 8 \cdot 2 \cdot 20 = 320$.

7. Sia p un primo. Dimostrare che ogni fattore primo q di $2^p - 1$ verifica $q > p$. Dedurre che esistono infiniti numeri primi.

   Sia q sia un fattore primo di $2^p - 1$. Quindi $2^p - 1 \equiv 0 \mod q$. Allora $o_q(2) \mid p$. Siccome $o_q(2) > 1$, allora, dato che p è primo, $o_q(2) = p$. D'altra parte $o_q(2) \mid q - 1$, quindi, in particolare, $p = o_q(2) \leq q - 1 < q$.

   Supponiamo per assurdo che i numeri primi siano finiti e sia $\overline{p}$ il più grande tra i numeri primi. Sappiamo però, per quanto visto sopra, che ogni divisore primo di $2^{\overline{p}} - 1$ è maggiore di $\overline{p}$. Ciò è un assurdo, perchè contraddice la massimalità di $\overline{p}$.

8. Sia $\sigma = (135)(26) \in S_6$ e $\tau = (16)(145) \in S_6$. Determinare $\sigma \circ \tau, \tau \circ \sigma, \tau^{-1}, \sigma^6, \tau^4$.

   $\sigma \circ \tau = (135)(26)(16)(145) = (14)(2635), \tau \circ \sigma = (16)(145)(135)(26) = (1362)(45)$. Notare che $\sigma \circ \tau$ e $\tau \circ \sigma$ sono diverse ma, scritte in cicli disgiunti, hanno la stessa struttura.

   $\tau^{-1} = (145)^{-1}(16)^{-1} = (541)(16) = (1654)$. Naturalmente si poteva prima scrivere τ come unico ciclo (1456) e poi invertirlo, ottenendo $(6541) = (1654)$.

   Dato che (135) e (26) sono permutazioni disgiunte, allora $\sigma^6 = (135)^6(26)^6 = ((135)^3)^2((26)^2)^3 = id_{S_6}$.

   $\tau^4 = (1456)^4 = id_{S_6}$. Notiamo che, invece, $(16)^4(145)^4 = (145)$.

9. Si consideri $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 7 & 6 & 3 & 1 & 2 \end{pmatrix} \in S_7$. Determinare σ^{-1}, scrivere σ come prodotto di cicli disgiunti e come prodotto di trasposizioni e quindi determinarne la parità.

   $$\sigma^{-1} = \begin{pmatrix} 4 & 5 & 7 & 6 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 5 & 1 & 2 & 4 & 3 \end{pmatrix}$$

   $\sigma = (146)(2537)$. $\sigma = (16)(14)(27)(23)(25)$. σ è una permutazione dispari.

10. Sia $n \geq 2$. Sia $A_n \subsetneq S_n$ l'insieme delle permutazioni pari. Dimostrare che $|A_n| = |S_n \setminus A_n|$ e che, quindi, $|A_n| = n!/2$.

    Sia $\tau \in S_n$ una qualsiasi trasposizione. Si consideri l'applicazione $f : A_n \to S_n \setminus A_n$ tale che $f(\rho) := \tau\rho$ per ogni $\rho \in A_n$. f è ben definita: se $\rho \in A_n$ allora $\tau\rho \in S_n \setminus A_n$. f è iniettiva, infatti se $\tau\rho = \tau\rho'$ allora $\rho = \rho'$. Inoltre f è suriettiva: se $\sigma \in S_n \setminus A_n$ allora $\tau\sigma \in A_n$ e $f(\tau\sigma) = \tau\tau\sigma = \sigma$. Perciò A_n e $S_n \setminus A_n$ hanno la stessa cardinalità. Siccome $S_n = A_n \cup (S_n \setminus A_n)$ e A_n e $S_n \setminus A_n$ sono chiaramente disgiunti, allora $|A_n| = |S_n|/2 = n!/2$.