Università degli Studi Roma Tre - Corso di Laurea in Matematica

Tutorato di AL110-19 Novembre 2010

A.A. 2010-2011 - Docente: Prof. Marco Fontana

Tutori: Cesare Catavitello e Alessandra Albanese

TUTORATO 6
19 NOVEMBRE 2010

1. Risolvere i seguenti sistemi di congruenze lineari:

   a) $\begin{cases} 2x \equiv 3 \pmod 5 \\ x \equiv 12 \pmod{11} \\ x \equiv 1 \pmod 7 \end{cases}$

   b) $\begin{cases} 3x \equiv 3 \pmod{10} \\ 3x \equiv 7 \pmod{11} \\ 11x \equiv 5 \pmod{21} \end{cases}$

   c) $\begin{cases} 6x \equiv 3 \pmod{13} \\ 2x \equiv 5 \pmod 7 \\ 81x \equiv 11 \pmod{34} \end{cases}$

   d) $\begin{cases} x \equiv 5 \pmod 6 \\ 5x \equiv 6 \pmod 7 \\ 9x \equiv 12 \pmod{23} \end{cases}$

   e) $\begin{cases} x \equiv -1 \pmod 9 \\ x \equiv 1 \pmod 5 \\ x \equiv -3 \pmod 4 \end{cases}$

2. Mostrare che presi comunque $a \in \mathbb{Z}$ e p un numero primo si ha che $a^p \equiv a \pmod p$.

3. Siano p e q due primi distinti. Per ogni $a \in \mathbb{Z}$, tale che $a^p \equiv a \pmod q$ e $a^q \equiv a \pmod p$, mostrare che $a^{pq} \equiv a \pmod{pq}$.

4. Mostrare che $\forall p, q$ primi distinti si ha che $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

5. Sia p un primo. Presi comunqe a,$b \in \mathbb{Z}$ mostrare che: $(a+b)^p \equiv a^p + b^p \pmod p$.

6. Mostrare che per ogni n fissato, $n \in \mathbb{N}$, $a_i \in \mathbb{Z}\ \forall i = 1, \ldots, n$ e p primo, si ha che : $(\sum_{i=1}^{n} a_i)^p \equiv \sum_{i=1}^{n} a_i^p \pmod p$.

7. Mostrare che, presi p e q primi distinti, si ha che $\forall a \in \mathbb{Z}$ si ha che $pq | (a^{pq} - a^q - a^p + a)$.

8. Mostrare che $\forall a \in \mathbb{Z}$ e $\forall m$,$n \in \mathbb{N}$ tali che $MCD(n, m) = 1$ si ha che $mn | a^{\varphi(n)\varphi(m)} + a^{\varphi(n)+1} - a - 1$ se e solo se $\varphi(n) | \varphi(m)$.

9. Dimostrare che $\forall n > 2 \in \mathbb{Z}\ \varphi(n) = 2k$, $k \in \mathbb{Z}$.

10. Dimostrare che $\forall p$ primo si ha che $\varphi(p) = p - 1$ e $\forall n \in \mathbb{Z}\, \varphi(p^n) = p^n - p^{n-1}$.

11. Trovare a_i tali che il seguente sistema abbia come soluzione $x \equiv 101 \pmod{420}$.
$$\begin{cases} x \equiv a_1 \pmod 5 \\ x \equiv a_2 \pmod 7 \\ x \equiv a_3 \pmod{12} \end{cases}$$

12. Esistono a_i tali che il sistema precedente non sia risolubile?

13. Trovare il più piccolo intero $a > 2$ tale che
$2|a$, $5|a + 3$, $6|a + 4$, $8|3a + 1$, $8|4a + 1$.