

Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2010/2011
TN410 - Introduzione alla teoria dei numeri
Tutorato 6 (5 maggio 2011)
Giacomo Milizia

1. Trovare il valore dei seguenti simboli di Legendre:

$$\left(\frac{43}{97}\right), \left(\frac{-187}{563}\right), \left(\frac{436}{977}\right), \left(\frac{3753}{641}\right), \left(\frac{-6045}{107}\right), \left(\frac{217}{863}\right).$$

2. Siano p, q numeri primi dispari distinti. Provare che: $\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right)$.

3. Stabilire quali delle seguenti congruenze quadratiche sono risolubili:

- (a) $X^2 \equiv 234 \pmod{577}$;
- (b) $3X^2 + 6X + 5 \equiv 0 \pmod{89}$;
- (c) $2X^2 + 5X - 9 \equiv 0 \pmod{179}$.

(577, 89 e 179 sono numeri primi).

4. Provare che:

- (a) se p e $q = 2p + 1$ sono entrambi numeri primi dispari, allora -4 è una radice primitiva di q ;
- (b) se $p \equiv 1 \pmod{4}$ è un numero primo, allora -4 e $\frac{p-1}{4}$ sono entrambi residui quadratici di p ;
- (c) se $p \equiv 7 \pmod{8}$ è un numero primo, allora p divide $2^{\frac{p-1}{2}} - 1$.

5. Stabilire se le seguenti congruenze quadratiche sono risolubili e, nei casi di risolubilità, trovare le soluzioni:

- (a) $X^2 \equiv 31 \pmod{3^3}$;
- (b) $X^2 \equiv 32 \pmod{7^2}$;
- (c) $X^2 \equiv 14 \pmod{5^3}$;
- (d) $X^2 + X + 1 \equiv 0 \pmod{7^2}$;
- (e) $X^2 + 6X + 2 \equiv 0 \pmod{3^3}$;
- (f) $X^2 \equiv 11 \pmod{2^{18}}$;
- (g) $X^2 \equiv 17 \pmod{2^5}$.

6. Determinare i numeri interi dispari a per i quali le seguenti congruenze sono risolubili ed, in corrispondenza ad essi, trovarne le soluzioni:

- (a) $X^2 \equiv a \pmod{2^4}$;
- (b) $X^2 \equiv a \pmod{2^5}$;
- (c) $X^2 \equiv a \pmod{2^6}$.