Zauważmy od razu, że tych rozwiązań jest co najwyżej p, bo tyle elementów ma pełny układ reszt modulo p. Możemy zakładać, że $n < p$, gdyż wobec 7.11 dla każdego $n \geqslant p$ istnieje takie $m < p$, że $x^n \equiv x^m \pmod{p}$ dla dowolnej liczby całkowitej x.

Przykład 8.3

1. $x^3 - 3 \equiv 0 \pmod{7}$ nie ma rozwiązań.
2. $x^{p-1} - 1 \equiv 0 \pmod{p}$ ma $p-1$ rozwiązań, co wynika z małego twierdzenia Fermata 7.9.

Twierdzenie 8.4 (**Lagrange**)
Kongruencja

$$a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}, \quad \textit{gdzie } (a_0, p) = 1,$$

ma co najwyżej n rozwiązań modulo p.

Dowód
Stosujemy indukcję ze względu na n. Dla $n = 1$ twierdzenie jest prawdziwe, bo $(a_0, p) = 1$. Załóżmy, że jest ono prawdziwe dla $n-1$.

Jeśli kongruencja

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{p} \tag{2}$$

nie ma rozwiązań, to teza jest prawdziwa. Załóżmy więc, że istnieje rozwiązanie x_1, czyli

$$a_0x_1^n + a_1x_1^{n-1} + \ldots + a_{n-1}x_1 + a_n \equiv 0 \pmod{p}. \tag{3}$$

Odejmując stronami (3) od (2), otrzymujemy

$$a_0(x^n - x_1^n) + a_1(x^{n-1} - x_1^{n-1}) + \ldots + a_{n-1}(x - x_1) \equiv 0 \pmod{p}. \tag{4}$$

Kongruencja (4) jest spełniona przez każde rozwiązanie kongruencji (2). Korzystając ze wzoru $x^k - x_1^k = (x - x_1)\,(x^{k-1} + x^{k-2}x_1 + \ldots + xx_1^{k-2} + x_1^{k-1})$, kongruencję (4) możemy zapisać w postaci

$$(x - x_1)\,(a_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) \equiv 0 \pmod{p}, \tag{5}$$

gdzie $b_1, b_2, \ldots, b_{n-1}$ są liczbami całkowitymi zależącymi tylko od x_1 oraz $a_0, a_1, \ldots, a_{n-1}$. Stąd każde rozwiązanie kongruencji (2) powinno albo spełniać kongruencję $x \equiv x_1 \pmod{p}$, albo być rozwiązaniem kongruencji

$$a_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1} \equiv 0 \pmod{p}.$$

Na mocy założenia indukcyjnego ostatnia kongruencja nie ma więcej niż $n-1$ rozwiązań, a więc kongruencja (2) nie ma więcej niż n rozwiązań, co dowodzi twierdzenia. □

Z twierdzenia Lagrange'a można otrzymać kryterium na to, kiedy liczba całkowita a jest tak zwaną resztą kwadratową modulo p.

Definicja 8.5
Niech p będzie liczbą pierwszą. Mówimy, że liczba całkowita a jest **resztą kwadratową modulo p** jeśli $(a,p)=1$ oraz istnieje liczba całkowita x taka, że $a \equiv x^2 \pmod{p}$. Jeśli kongruencja ta nie ma rozwiązania, to liczbę a nazywamy **niereszą kwadratową modulo p**.

Twierdzenie 8.6 (**Euler**)
Niech p będzie liczbą pierwszą nieparzystą i $a \in \mathbb{Z}$. Kongruencja

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

jest prawdziwa wtedy i tylko wtedy, gdy a jest resztą kwadratową modulo p.

Dowód
Przypuśćmy, że istnieje x takie, że $a \equiv x^2 \pmod{p}$. Wtedy $(x,p)=1$, bo $(a,p)=1$. Podnosząc obie strony ostatniej kongruencji do potęgi $\frac{p-1}{2}$, otrzymujemy

$$x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Z twierdzenia Fermata wiemy, że $x^{p-1} \equiv 1 \pmod{p}$, a więc $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Na odwrót, załóżmy, że kongruencja $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ jest prawdziwa. Z twierdzenia Lagrange'a (twierdzenie 8.4) wiadomo, że kongruencja $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ może mieć co najwyżej $\frac{p-1}{2}$ rozwiązań modulo p. Ale istnieje dokładnie $\frac{p-1}{2}$ reszt kwadratowych spełniających to równanie, a mianowicie

$$1^2, 2^2, 3^2, \ldots, \left(\tfrac{p-1}{2}\right)^2.$$

Rzeczywiście, liczby te nie przystają do siebie modulo p, bo jeśli $r \neq s$ i $r^2 \equiv s^2 \pmod{p}$, to albo $r \equiv s$, albo $r \equiv -s \pmod{p}$, ale nie jest to możliwe, gdyż $1 \leqslant r, s \leqslant \frac{p-1}{2}$. Wynika stąd, że kongruencja $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ma tylko rozwiązania będące resztami kwadratowymi, co kończy dowód twierdzenia. □

Następne twierdzenie o kongruencjach jest trochę innego typu niż poprzednie. Ma ono charakter bardziej ogólny w tym sensie, że może być przeformułowane na twierdzenie o własności ideałów w pierścieniu.

Twierdzenie 8.7 (**chińskie twierdzenie o resztach**)
Niech n będzie liczbą naturalną $n \geqslant 2$, zaś $m_1, m_2, \ldots, m_n$ układem n liczb naturalnych, takich że $(m_i, m_j)=1$ dla $i \neq j$, oraz $a_1, a_2, \ldots, a_n$ dowolnym układem n liczb całkowitych. Wówczas istnieje wspólne rozwiązanie kongruencji

$$x \equiv a_i \pmod{m_i} \text{ dla } i = 1, 2, \ldots, n.$$

Rozwiązanie to jest jedyne modulo $m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

Dowód
Oznaczmy $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$. Ponieważ $(\frac{m}{m_i}, m_i) = 1$, więc na mocy twierdzenia 4.2 istnieje liczba x_i taka, że

$$\frac{m}{m_i} x_i \equiv 1 \pmod{m_i}.$$