Chapter 4 of Number Theory with Computer Applications

by Kumanduri and Romero;

University of Windsor MATH 3270 Course notes by M. Hlynka

and W.L. Yee.

FUNDAMENTAL THEOREMS OF MODULAR ARITHMETIC

4.1 FERMAT'S THEOREM:

Theorem 4.1.1 Fermat's Little Theorem: let p be a prime.

(a) Then $a^p \equiv a \pmod{p}$ for all integers a.

(b) If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof.

(a) WLOG assume that $a > 0$.

Version 1: Induction. Show $n^p \equiv n \pmod{p}$. This is true for $n = 1$. Assume it is true for fixed n. Show it is true for $n + 1$.

$$\begin{aligned}(n+1)^p &\equiv n^p + \binom{p}{1} n^{p-1} 1^1 + \binom{p}{2} n^{p-2} 1^2 + \cdots + \binom{p}{p} n^0 1^p \\ &\equiv n^p + 1 \text{ since the other terms are divisible by } p \\ &\equiv n + 1 \bmod p \text{ (by induction).}\end{aligned}$$

The other terms are divisible by p since $\binom{p}{i} = \dfrac{p!}{i!(p-i)!}$. Note that the numerator is divisible by p but the denominator has no terms involving p except when $i = 0, p$ so $p | \binom{p}{i}$ for $i = 1, \ldots, p-1$. ■

Proof. Version 2:

Clearly $\{0, 1, \ldots, p-1\}$ is a complete residue system (mod p). We show that $\{0, a, \ldots, a(p-1)\}$ is also a complete residue system (mod p) for $(a, p) = 1$.

Suppose $ax \equiv ay \pmod{p}$ for $x, y \in \{0, \ldots, p-1\}$. Then $p|(ax-ay)$ so $p|a(x-y)$ so $p|(x-y)$ so $x \equiv y \pmod{p}$. So $\{0, a, \ldots, a(p-1)\}$ is a complete residue system $\pmod{p}$. Thus
$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} ai \equiv a^{p-1} \prod_{i=1}^{p-1} i \pmod{p}$.
Since $(\prod_{i=1}^{p-1} i, p) = 1$, we can cancel $\prod_{i=1}^{p-1} i$ from both sides to get $a^{p-1} \equiv 1 \pmod{p}$ so $a^p \equiv a \pmod{p}$.
This assumes $(a, p) = 1$. If $(a, p) \neq 1$ then $p|a$ so $a^p \equiv a \pmod{p}$ as well.
(b) From $a^p \equiv a \pmod{p}$ we get $a^p - a \equiv a(a^{p-1} - 1) \equiv 0 \pmod{p}$. Since $p \not| a$, therefore $a^{p-1} \equiv 1 \pmod{p}$. ■

NOTE This theorem gives us a way to find the inverse of a mod p if $(a, p) = 1$. Since $a^{p-1} \equiv 1$ mod p, we see that $a(a^{p-2}) \equiv 1$ mod p so a^{p-2} is the inverse of a mod p.

Example Show that $S = 1^{47} + 2^{47} + 3^{47} + 4^{47} + 5^{47} + 6^{47}$ is a multiple of 7. (from 1001 Problems in Classical Number Theory, by De Koninck and Mercier, p. 19)
SOLUTION: By Fermat's Little Theorem, $a^6 \equiv 1 \mod 7$.

$$2^{47} \equiv 2^{42}2^5 \equiv (2^6)^7 2^5 \equiv 1^7 2^5 \equiv 2^5 \equiv 2^6 a_2 \equiv a_2 \pmod{7}$$

where a_2 is the inverse of 2 mod 7.
Thus $S \equiv 1 + a_2 + a_3 + a_4 + a_5 + a_6$ mod 7. Note that $1, a_2, a_3, \ldots, a_6$ along with 0 form a complete residue system modulo 7. Since the a_i are invertible, they are non-zero. 1 is the inverse of itself. If, for example, $a_2 = a_3$, then $2a_2 3 = 1 \cdot 3 = 2 \cdot 1$ so $2 = 3$ modulo 7–contradiction. Therefore $S \equiv 1 + a_2 + a_3 + a_4 + a_5 + a_6 \equiv 1 + 2 +$

$\cdots + 6 \equiv 0 \pmod 7$..

Example Show $7 \nmid n^2 + 1$ for any n.

SOLUTION: Case 1: If $7|n$, then $7|n^2$ so $7 \nmid n^2 + 1$.

Case 2. $(7, n) = 1$. Suppose $n^2 + 1 \equiv 0$ mod 7. Then $n^2 \equiv -1$ mod 7 and cubing both sides gives $n^6 \equiv -1$ mod 7. But by Fermat's Little Theorem, $n^6 \equiv 1$ mod 7. Contradiction. So $n^2 + 1 \not\equiv 0$ mod 7 so $7 \nmid n^2 + 1$.

Exercises p. 105 of text.

1. Find the remainder when 2^{372} is divided by 37.

$2^{372} \equiv (2^{36})^{10} 2^{12} \equiv 2^{12} \pmod{37}$.

$2^4 \equiv 16 \pmod{37}$

$2^8 \equiv 16^2 \equiv 256 \equiv 34 \pmod{37}$.

$2^{372} \equiv 2^8 \cdot 2^4 \equiv 34 \cdot 16 \equiv 544 \equiv 26 \pmod{37}$.

2. Prove that $11 \not| n^2 + 1$ for any integer$n$.

Assume $11|n^2 + 1$ for some n, then $n^2 \equiv -1 \mod 11$, and $n^{10} \equiv (-1)^5 \equiv -1 \mod 11$. If $11|n$ then $11|n^2$ so 11 cannot divide $n^2 + 1$. If $11 \nmid n$, then $(11, n) = 1$ so by Fermat's Little Theorem, $n^{10} \equiv 1$ mod 11. Contradiction. Thus $11 \nmid n^2 + 1$.

Proposition 4.1.5 (p. 106)

Suppose $a^r \equiv 1 \pmod p$ and p is prime. Let $d = (r, p - 1)$. Then $a^d \equiv 1$ mod p.

Proof. $d = ur + v(p - 1)$ since $d = (r, p - 1)$. Thus

$$a^d \equiv a^{ur+v(p-1)} \equiv a^{ur} a^{v(p-1)} \equiv (a^r)^u (a^{p-1})^v \equiv (1)(1) \equiv 1 \pmod p.$$

Note that this makes sense even though one of u and v is negative.

■

Exercises p. 107 #1,2,3,4,7,8,9

Exercise p. 107 # 3) Show that if $n \equiv 2 \pmod 4$, then $9^n + 8^n$ is divisible by 5.

n is of the form $n = 4k + 2$. Then

$9^n + 8^n \equiv 9^{4k+2} + 8^{4k+2} \equiv (9^4)^k \cdot 9^2 + (8^4)^k \cdot 8^2 \equiv 81 + 64 \equiv 0 \pmod 5$

where $9^4 \equiv 8^4 \equiv 1 \pmod 5$ by Fermat's Little Theorem.

Andreescu, Andrica, Feng 104 Number Theory Problems From the Training of the USA IMO Team

Example 1.29: Let p be prime. Prove that p divides $ab^p - ba^p$ for all integers a and b.

By Fermat's Little Theorem, $a^p \equiv a \pmod p$ and $b^p \equiv b \pmod p$. Therefore $ab^p - ba^p \equiv ab - ba \equiv 0 \pmod p$.

Exercise p. 107 # 4) For which values of n is $3^n + 2^n$ divisible by 7?

By Fermat's Little Theorem, $3^{n+6k} \equiv 3^n \pmod 7$ and $2^{n+6k} \equiv 2^n \pmod 7$, so the value of $3^n + 2^n \pmod 7$ cycles with cycle length 6.

$n \pmod 6$	$3^n + 2^n \pmod 7$
0	$1 + 1 \equiv 2$
1	$3 + 2 \equiv 5$
2	$9 + 4 \equiv 6$
3	$27 + 8 \equiv 0$
4	$81 + 16 \equiv 6$
5	$243 + 32 \equiv 2$
6	$729 + 64 \equiv 2$

The non-negative integers n for which $3^n + 2^n$ is divisible by 7 are all n of the form $6k + 3$.

4.2 The Euler Phi Function p. 107

"Euler" is pronounced "Oiler" (as in the Edmonton hockey team). Euler was a Swiss mathematician, perhaps the most creative and prolific, of all time.

Definition 4.2.1 Let $\phi(m)$ be the number of invertible elements in a complete residue system mod m. This is called the Euler phi function.

Alternatively, $\phi(m)$ is the number of positive integers less than or equal to m which are relatively prime to m (i.e. whose gcd with m is 1).

Example

A complete residue system mod 6 is $\{0, 1, 2, 3, 4, 5\}$. The invertible elements are those which are relatively prime to 6, namely $\{1, 5\}$. So $\phi(6) = 2$.

The invertible elements mod 8 are $\{1, 3, 5, 7\}$ so $\phi(8) = 4$.

If p is prime, then the invertible elements mod p are $\{1, 2, \ldots, p-1\}$ so $\phi(p) = p - 1$.

Property p. 108

If p is a prime and r is a positive integer, then $\phi(p^r) = p^r\left(1 - \frac{1}{p}\right)$.

Proof. Consider the complete residue system $S = \{1, 2, \ldots, p^r\}$. In order to be not relatively prime to p^r, an integer must be a multiple of p. These multiples are $p, 2p, 3p, \ldots, p^{r-1}, (p^{r-1})p$. So there are p^{r-1} of them. The number of elements in S relatively prime to p^r is $p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$. ■

Theorem 4.2.3 p.108 If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. Let S_r be a standard residue system mod r, i.e. $S_r = \{1, \ldots, r\}$, for $r = m, n, mn$. Let U_r be the invertible elements of S_r.

Then $k \longleftrightarrow (a, b)$ where $k \in U_{mn}$ and $a \in U_m$ and $b \in U_n$ for the following reason.

(a) Given $k \in U_{mn}$, we have $(k, mn) = 1$ so $(k, m) = 1$ so $k \equiv a \mod m$ for some $a \in U_m$. Similarly, $k \equiv b \mod n$ for some $b \in U_n$.

(b) Conversely, given $a \in U_m$ and $b \in U_n$, we use the Chinese Remainder Theorem to find $k \in U_{mn}$ such that $k \equiv a \mod m$, and $k \equiv b \mod n$.

This one to one correspondence gives us that

$\phi(mn) = \#U_{mn} = \#U_m \#U_n = \phi(m)\phi(n)$. ∎

Illustration of above theorem

$m = 3$, $n = 4$. $mn = 12$. Then $U_m = \{1, 2\}$, $U_n = \{1, 3\}$, $U_{mn} = \{1, 5, 7, 11\}$. A value from U_{mn}, say 11, will give $11 \equiv 2 \pmod{m}$ so $a = 2$, and $11 \equiv 3 \pmod{n}$ so $b = 3$. Thus $11 \to (2, 3)$. Conversely, consider a pair from U_m and U_n, say (2,1). Solve $x \equiv 2 \mod 3$ and $x \equiv 1 \mod 4$. Using the Chinese Remainder Theorem, we there exists a unique solution $x \equiv 5 \mod 12$. We get the correspondence

$(1, 1) \leftrightarrow 1$, $(1, 3) \leftrightarrow 7$, $(2, 1) \leftrightarrow 5$, $(2, 3) \leftrightarrow 11$. Thus $\#U_{mn} = \#U_m \#U_n$.

Corollary 4.2.4 If $m = p_1^{a_1} \ldots p_k^{a_k}$ is the prime factorization of m, then

$$\phi_(m) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Proof.

$$\begin{aligned}\phi(m) &= \phi(p_1^{a_1} \dots p_k^{a_k}) = \phi(p_1^{a_1}) \dots \phi(p_k^{a_k}) \\ &= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \dots p_k^{a_k}\left(1 - \frac{1}{p_k}\right) = p_1^{a_1} \dots p_k^{a_k}\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) \\ &= m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)\end{aligned}$$

■

Example: How many positive integers are less than 180 and relatively prime to it?

SOLUTION: $\phi(180) = \phi(2^2 3^2 5) = 180(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 180(1/2)(2/3)(4/5) = 48$.

Example: Find all n such that $\phi(n) = n - 3$.

SOLUTION: If $n = p^a$, then $n - 3 = \phi(n) = n(1 - (1/p)) = n - (n/p) = n - p^{a-1}$ so

$p^{a-1} = 3$. Thus $p = 3$ and $a - 1 = 1$ so $a = 2$. Hence $n = 3^2 = 9$.

If $n = p_1^{a_1} p_2^{a_2}$, then $n - 3 = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) = n - n(\frac{1}{p_1} + \frac{1}{p_2}) + \frac{n}{p_1 p_2}$.

Thus

$3 = \frac{n}{p_1} + \frac{n}{p_2} - \frac{n}{p_1 p_2} = p_1^{a_1-1} p_2^{a_2} + p_1^{a_1} p_2^{a_2-1} - p_1^{a_1-1} p_2^{a_2-1} = p_1^{a_1-1} p_2^{a_2-1}(p_2 + p_1 - 1)$. But p_1 and p_2 are distinct primes so the smallest $p_2 + p_1 - 1$ can be is $2 + 3 - 1 = 4$ which is larger than 3. Hence the only solution is $n = 9$.

Exercises p. 110. 1,3,4,5,6,8.

Exercise p. 110 # 8) Prove that if $\phi(n) | n - 1$, then n is squarefree.

Let $n = p_1^{a_1} \cdots p_k^{a_k}$. Note that $(n-1, n) = 1$ so $p_i \nmid \phi(n)$ for $i = 1, \ldots, k$.

$$\phi(n) = p_1^{a_1} \cdots p_k^{a_k} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

so in order for $\phi(n)$ to be not divisible by p_i, $a_i = 1$. Therefore n is squarefree.

4.3 EULER'S THEOREM p. 112

Euler's Theorem If a and m are integers with $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof. Let $S_1 = \{r_1, \ldots, r_{\phi(m)}\}$ be a reduced residue system, i.e. a residue system containing every invertible element (mod m). Consider $S_2 = \{ar_1, \ldots, ar_{\phi(m)}\}$. Since a is invertible and r_i is invertible, then ar_i is invertible (since it is relatively prime to m). Furthermore, $ar_i \equiv ar_j \pmod{m}$ if and only if $r_i \equiv r_j$ since a is invertible. Thus $S_1 \equiv S_2 \mod m$ but perhaps in a different order. So $\prod_{i=1}^{\phi(m)} r_i \equiv \prod_{i=1}^{\phi(m)} ar_i \equiv a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i \mod m$. Hence $a^{\phi(m)} \equiv 1 \pmod{m}$. ■

Example Find the last three digits of 2009^{2009}.

SOLUTION: We want $2009^{2009} \pmod{1000}$. First $1000 = 2^3 5^3$. Thus $\phi(1000) = \phi(2^3 5^3) = 1000(1 - 1/2)(1 - 1/5) = 400$. So $2009^{2009} \equiv 2009^{2000} 2009^9 \equiv (2009^{400})^5 9^9 \equiv (1) 9^9 \mod 1000$.

But

$$\begin{aligned} 9^9 &= 81 \cdot 81 \cdot 81 \cdot 81 \cdot 9 = 6561 \cdot 6561 \cdot 9 \equiv 561 \cdot 561 \cdot 9 \equiv 314721 \cdot 9 \\ &\equiv 721 \cdot 9 \equiv 6489 \equiv 489 \mod 1000. \end{aligned}$$

Example

Improving Euler's theorem. Find the remainder when 163^{199} is divided by 108.

Solution: (163,108)=1 so $163^{\phi(108)} \equiv 1 \mod 108$. But $\phi(108) = \phi(4(27)) = \phi(2^2 3^3) = 108(1-1/2)(1-1/3) = 36$. So Euler's theorem gives $163^{36} \equiv 1 \mod 108$. Now $\phi(27) = 27(1-1/3) = 18$, and $\phi(4) = 2$. Thus by Euler's Theorem, $163^{18} \equiv 1 \mod 27$ and $163^2 \equiv 1 \mod 4$. Raising both sides to the ninth power gives $163^{18} \equiv 1 \mod 4$.

Since $163^{18} \equiv 1 \mod 27$ and $163^{18} \equiv 1 \mod 4$, it follows that $163^{18} \equiv 1 \mod 108$. We have improved by dropping the power from 36 to 18.

Hence $163^{199} \equiv (163^{18})^{11} 163 \equiv (1)(55) \equiv 5 \mod 108$. So the remainder is 55.

Testing for nonPrimes If we do not know if m is prime or not, we can choose a such that $(a, m) = 1$ and compute $a^{m-1} \mod m$. If $a^{m-1} \not\equiv 1 \mod m$, then m is not prime.

Example: Prove that 341 is not prime by computing $3^{340} \pmod{341}$.

Check: $2^8 + 2^6 + 2^4 + 2^2 = 340$.

Consider $3^{340} \equiv 3^{2^8+2^6+2^4+2^2} \equiv 3^{2^8} 3^{2^6} 3^{2^4} 3^{2^2} \mod 341$.

$3^{2^0} \equiv 3 \mod 341$

$3^{2^1} \equiv 3^2 \equiv 9 \mod 341$

$3^{2^2} \equiv 3^4 \equiv 9^2 \equiv 81 \mod 341$

$3^{2^3} \equiv 3^8 \equiv 81^2 \equiv 6561 \equiv 82 \mod 341$

$3^{2^4} \equiv 3^{16} \equiv 82^2 \equiv 6724 \equiv 245 \mod 341$

$3^{2^5} \equiv 3^{32} \equiv 245^2 \equiv 60025 \equiv 9 \mod 341$

$3^{2^6} \equiv 3^{64} \equiv 9^2 \equiv 81 \bmod 341$

$3^{2^7} \equiv 3^{128} \equiv 81^2 \equiv 82 \bmod 341$

$3^{2^8} \equiv 3^{256} \equiv 82^2 \equiv 245 \bmod 341$

Thus

$$\begin{aligned} 3^{340} &\equiv 3^{2^8} 3^{2^6} 3^{2^4} 3^{2^2} \equiv (245)(81)(245)(81) \\ &\equiv (245)(245)(81)(81) \equiv (9)(82) \equiv 738 \equiv 56 \bmod 341 \ . \end{aligned}$$

Conclusion: 341 is not prime (because $3^{340} \not\equiv 1 \bmod 341$.

Exercises p. 116 #1,3,4,5,6,10,11.

Using Euler's Theorem twice, find the last two digits of $7^{13^{100}}$.

I.e. find the remainder modulo 100.

$(7, 100) = 1$ and $\phi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$ so $7^{40} \equiv 1 \pmod{100}$, so we wish to find $13^{100} \pmod{40}$.

$(13, 40) = 1$ and $\phi(40) = 40\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 16$ so $13^{16} \equiv 1 \pmod{40}$. Thus

$13^{100} \equiv 13^{16 \cdot 6+4} \equiv (13^{16})^6 \cdot 13^4 \equiv 13^4 \equiv (169)^2 \equiv 9^2 \equiv 1 \pmod{40}$.

Let $13^{100} = 40k + 1$. Therefore

$7^{13^{100}} \equiv 7^{40k+1} \equiv (7^{40})^k \cdot 7 \equiv 7 \pmod{100}$.

Therefore the last two digits are 07.

Exercise p. 116 # 3) Use Euler's Theorem and the Chinese Remainder Theorem to show that $n^{12} \equiv 1 \pmod{72}$ for all $(n, 72) = 1$.

$\phi(8) = 4$ so $n^4 \equiv 1 \pmod 8$ for $(n, 8) = 1$.

$\phi(9) = 9\left(1 - \frac{1}{3}\right) = 6$ so $n^6 \equiv 1 \pmod 9$ for all $(n, 9) = 1$.

Therefore $n^{12} \equiv 1 \pmod 8$ and $n^{12} \equiv 1 \pmod 9$ for $(n, 72) = 1$, and thus by the Chinese Remainder Theorem $n^{12} \equiv 1 \pmod{72}$ for

$(n, 72) = 1$.

Exercise p. 116 # 5) Prove that $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$ if $(m, n) = 1$.

$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{m}$ by Euler's Theorem.

$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{n}$ by Euler's Theorem.

Therefore by the Chinese Remainder Theorem $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$.

Exercise p. 116 # 10) Prove that $a^{560} \equiv 1 \pmod{561}$ for all $(a, 561) = 1$.

$561 = 3 \times 11 \times 17$

$a^2 \equiv 1 \pmod{3}$ for $(a, 3) = 1$.

$a^{10} \equiv 1 \pmod{11}$ for $(a, 11) = 1$.

$a^{16} \equiv 1 \pmod{17}$ for $(a, 17) = 1$.

$2, 10, 16$ all divide 560. Therefore

$a^{560} \equiv 1 \pmod{3}$ for $(a, 3) = 1$. $a^{560} \equiv 1 \pmod{11}$ for $(a, 11) = 1$. $a^{560} \equiv 1 \pmod{17}$ for $(a, 17) = 1$. Therefore by the Chinese Remainder Theorem, $a^{560} \equiv 1 \pmod{561}$ for $(a, 561) = 1$.

Adreescu, Andrica, Feng 104 Number Theory Problems From the Training of the USA IMO Team

Example 1.30: Let $p \geq 7$ be prime. Prove that the number $\underbrace{11\cdots 1}_{p-1\ 1\text{'s}}$ is divisible by p.

$\underbrace{11\cdots 1}_{p-1\ 1\text{'s}} = \frac{10^{p-1}-1}{9}$ and $(10, p) = 1$ and $(9, p) = 1$, thus the conclusion follows from Fermat's Little Theorem.

4.4 LAGRANGE'S THEOREM Fundamental Theorem of Algebra: Over the real numbers, a polynomial of degree n has at most n real roots. Over the complex numbers, a polynomial of degree n has exactly n complex roots counting multiplicity.

Similar theorem holds for prime modulus, but not for composite modulus.

Lagrange's Theorem: Let p be a prime number, and let $f(x)$ be a polynomial of degree $n \geq 1$, not all of whose coefficients are divisible by p. Then $f(x) \equiv 0 \pmod{p}$ has at most n solutions in a complete residue system modulo p.

Proof: Use induction on degree of $f(x)$.

Base case: $\deg f(x) = 1$. Then $f(x) = ax+b$. If $p \nmid a$, then $ax+b \equiv 0 \pmod{p}$ has a unique solution modulo p. If $p|a$ and $p \nmid b$, then there is no solution. In both cases, there is at most one solution. Note that we can't have $p|a$ and $p|b$ since not all coefficients of f are divisible by p.

Induction hypothesis: assume that for all polynomials of degree less than n as in the statement of the theorem the number of solutions is at most the degree of the polynomial.

Induction step: Let $f(x)$ be a polynomial of degree n as in the statement of the theorem. If $f(x)$ has no roots, we are done. If $f(x)$ has a root, let a be a root. By the Division Theorem for polynomials, there exist $q(x)$ and $r(x)$ such that

$$f(x) = (x-a)q(x) + r(x) \qquad \text{and } \deg r(x) < \deg (x-a).$$

Thus $r(x)$ is a constant which we denote by r.

Substituting $x = a$ and $f(a) \equiv 0 \pmod{p}$, we see that $r \equiv 0 \pmod{p}$. Thus $f(x) \equiv (x-a)q(x) \pmod{p}$. $q(x)$ is a polynomial of degree at most $n-1$ not all of whose coefficients are divisible by p. Therefore q has at most $n-1$ roots by the induction hypothesis.

If a is not a root of $q(x)$, consider a root b of $f(x)$. $b = a$ or b is a root of $q(x)$ because $f(b) \equiv (b-a)q(b) \equiv 0 \pmod{p}$ and $b-a$ is invertible mod p forcing $q(b) \equiv 0 \pmod{p}$. By the induction hypothesis, q has at most $n-1$ roots so f has at most n roots.

If a is a root of $q(x)$, divide $q(x)$ by the highest power of $x-a$ possible and write $f(x) \equiv (x-a)^k q'(x)$ where $q'(a) \not\equiv 0 \pmod{p}$. q' has degree $n-k$ and so has at most $n-k$ roots by the induction hypothesis. If b is a root of f and $b \not\equiv a$, then $f(b) \equiv (b-a)^k q'(b) \equiv 0 \pmod{p}$. Again, $b-a$ is invertible mod p so we must have $q'(b) \equiv 0 \pmod{p}$. Every root of f different from a must be a root of q' and there are $n-k$ of these. Therefore f has at most n roots.

Eg. $x^3 \equiv 8 \pmod{13}$ has three solutions: $x \equiv 2, 5, 6 \pmod{13}$.
Eg. $x^2+3x+4 \equiv 0 \pmod{7}$ has at most two solutions by Lagrange's Theorem. $x \equiv 2 \pmod{7}$ is the only solution to the congruence:

x	$x^2+3x+4 \pmod{7}$
0	4
1	$8 \equiv 1$
2	$14 \equiv 0$
3	$22 \equiv 1$
4	$32 \equiv 4$
5	$44 \equiv 2$
6	$58 \equiv 2$

Corollary 4.4.3: Let p be a prime and $d | p-1$. Then the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.

Proof: By Fermat's Little Theorem, $x^{p-1} \equiv 1 \pmod{p}$ for all $(x, p) = 1$. Thus the congruence has $p-1$ solutions. Let $p-1 = dk$. Then

$$x^{p-1} - 1 = (x^d - 1)(x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1).$$

By Lagrange's Theorem, $x^d - 1 \equiv 0 \pmod{p}$ has at most d solutions and $x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1 \equiv 0 \pmod{p}$ has at most $d(k-1)$ solutions. The right hand side has at most $d + d(k-1) = dk = p-1$ solutions, but the left hand side has exactly $p-1$ solutions. Thus each polynomial factor on the right hand side must have the maximum number of solutions possible. Thus $x^d \equiv 1 \pmod{p}$ has d solutions when $d|p-1$.

Eg. If p is a prime such that $p \equiv 1 \pmod{4}$, then $x^2 \equiv -1 \pmod{p}$ has a solution.

Proof: Let $p = 4k+1$. By Fermat's Little Theorem, the equation $x^{4k} \equiv 1 \pmod{p}$ has $4k$ solutions in a complete residue system. Factor:

$$x^{4k} - 1 = (x^{2k} - 1)(x^{2k} + 1) \pmod{p}.$$

Every root of the left hand side is a root of either $x^{2k} - 1 \equiv 0 \pmod{p}$ or $x^{2k} + 1 \equiv 0 \pmod{p}$. By Corollary 4.4.3, $x^{2k} - 1 \equiv 0$ has exactly $2k$ solutions. Therefore $x^{2k} + 1 \equiv 0 \pmod{p}$ has exactly $2k$ solutions. If a is a root, then $(a^k)^2 \equiv -1 \pmod{p}$ so a^k is a solution to the congruence $x^2 \equiv -1 \pmod{p}$.