1 Exercises

1.1

Verify that the theorem is true for $a = 2$ and $p = 5$.

$2^{5-1} = 16 = 3 * 5 + 1 \equiv 1 \pmod 5$.

1.2

Calculate 2^2 and $20^{10} \pmod{11}$.

$$\begin{aligned}
2^2 &\equiv 4 \pmod{11}\\
2^4 &\equiv 5 \pmod{11}\\
2^8 &\equiv 3 \pmod{11}\\
2^2 * 2^8 &\equiv 1 \pmod{11}
\end{aligned}$$

1.3

What are the pairs when $p = 11$?

(2, 6), (3, 4), (5, 9), (6, 2), (7, 8).

2 Problems

2.1

What is the least residue of

$$5^6 \pmod 6, \quad 5^8 \pmod 7, \quad 1945^8 \pmod 7$$

$$5^2 \equiv 4 \pmod 7$$
$$5^4 \equiv 2 \pmod 7$$
$$5^6 \equiv 1 \pmod 7,$$
$$5^8 \equiv 4 \pmod 7,$$
$$1945 \equiv 545 \equiv 195 \equiv 55 \equiv 6 \pmod 7$$
$$1945^2 \equiv 1 \pmod 7$$
$$1945^8 \equiv 1 \pmod 7$$

2.2

What is the least residue of

$$5^{10} \pmod{11}, \quad 5^{12} \pmod{11}, \quad 1945^{12} \pmod{11}$$

$$5^2 \equiv 3 \pmod{11}$$
$$5^4 \equiv 9 \pmod{11}$$
$$5^8 \equiv 4 \pmod{11}$$
$$5^1 0 \equiv 1 \pmod{11},$$
$$5^1 2 \equiv 3 \pmod{11},$$
$$1945 \equiv 845 \equiv 75 \equiv 9 \pmod{11}$$
$$1945^2 \equiv 4 \pmod{11}$$
$$1945^4 \equiv 5 \pmod{11}$$
$$1945^8 \equiv 3 \pmod{11}$$
$$1945^{12} \equiv 4 \pmod{11}$$

2.3

What is the last digit of 7^{355}?

$$7 \equiv 7 \pmod{10}$$
$$7^2 \equiv 9 \pmod{10}$$
$$7^4 \equiv 1 \pmod{10}$$
$$355 \equiv 35 \equiv 3 \pmod{4}$$
$$7^{355} \equiv 7 * 9 \equiv 3 \pmod{10}$$

So, the last digit is 3.

2.4

What are the last two digits of 7^{355}?

$$7 \equiv 7 \pmod{100}$$
$$7^2 \equiv 49 \pmod{100}$$
$$7^4 \equiv 1 \pmod{100}$$
$$7^{355} \equiv 7 * 49 \equiv 43 \pmod{10}$$

2.5

What is the remainder when 314^{162} is divided by 163?
Since 163 is prime, by Fermat's Theorem, $314^{162} \equiv 1 \pmod{p}$.

2.6

What is the remainder when 314^{162} is divided by 7?

$$314 \equiv 6 \pmod{7}$$
$$314^2 \equiv 1 \pmod{7}$$
$$314^162 \equiv 1 \pmod{7}$$

2.7

What is the remainder when 314^{164} is divided by 165?
The prime decomposition of 165 is $3 * 5 * 11$.

$$314 \equiv 2 \pmod{3}$$
$$314^2 \equiv 1 \pmod{3}$$
$$314^{164} \equiv 1 \pmod{3},$$
$$314 \equiv 4 \pmod{5}$$
$$314^2 \equiv 1 \pmod{5}$$
$$314^{164} \equiv 1 \pmod{5},$$
$$314 \equiv 6 \pmod{11}$$
$$314^2 \equiv 3 \pmod{11}$$
$$314^4 \equiv 9 \pmod{11}$$
$$314^8 \equiv 4 \pmod{11}$$
$$314^{16} \equiv 5 \pmod{11}$$
$$314^{32} \equiv 3 \pmod{11}$$
$$314^{64} \equiv 9 \pmod{11}$$
$$314^{128} \equiv 4 \pmod{11}$$
$$314^{164} \equiv 4 * 3 * 9 \equiv 9 \pmod{11}.$$

Now have to solve the system of congruences:

$$x \equiv 1 \pmod{15}, \quad x \equiv 9 \pmod{11}$$

Solving:

$$\begin{aligned} 15k_1 + 1 &\equiv 9 \pmod{11} \\ k_1 &\equiv 2 \pmod{11} \\ x &\equiv 31 \pmod{165} \end{aligned}$$

So, the remainder is 31.

2.8

What is the remainder when 2001^{2001} is divided by 26?

$$\begin{aligned} 2001 &\equiv 25 \pmod{26} \\ 2001^2 &\equiv 1 \pmod{26} \\ 2001^{2001} &\equiv 25 \pmod{26} \end{aligned}$$

2.9

Show that

$$(p-1)(p-2)...(p-r) \equiv (-1)^r r! \pmod{p}$$

for $r = 1, 2, ..., p-1$.

Expanding the product $(p-1)(p-2)...(p-r)$, notice that all terms will be a multiple of p other than the product of $-1 * -2 * ... * -r = (-1)^r r!$.

2.10

(a) Calculate $(n-1)! \pmod{n}$ for $n = 10, 12, 14$, and 15.
(b) Guess a theorem and prove it.

(a) Since $2|9!$ and $5|9!$, then $9! \equiv 0 \pmod{10}$. Likewise, since 2 and 6 divide $11!$, $11! \equiv 0 \pmod{12}$; since 7 and 2 divide $13!$, $13! \equiv 0 \pmod{14}$; and since 3 and 5 divide $14!$, $14! \equiv 0 \pmod{15}$.
(b) For any composite, non-square n, $n|(n-1)!$. If n is composite, can write it as ab, with $a, b \in [2, n-1]$. Since $a \neq b$, then these a and b must be one of the products of $(n-1)! = 1 * 2 * ... * a * ... * b * ... * n-1$. The property doesn't hold for square $n = 4$, as $4 \nmid 6$. Writing $n = a^2$, it clearly holds for $a = 3$, as $3 * 6|8!$, so $9|8!$. So it will hold as long as a and $2a$ are products of $(a^2-1)!$. This is true if $2a < a^2 - 1$, or $a^2 - 2a - 1 > 0$. For $a = 3$, $9 - 6 - 1 > 0$. The derivative of this function with respect to a is $2a - 2$, which is non-negative for all $a \geq 0$. So all $a \geq 3$ will fulfill the equation.

2.11

Show that $2(p-3)! + 1 \equiv 0 \pmod{p}$.

Equivalently, we want to show that $2(p-3)! \equiv -1 \pmod{p}$. From Wilson's Theorem, we know that $(p-1)! \equiv -1 \pmod{p}$, so if we show that $2(p-3)! \equiv (p-1)! \pmod{p}$, we will be done. Notice that $(p-1)! = (p-1)(p-2)(p-3)!$. $(p-1)(p-2) \equiv 2 \pmod{p}$, so $(p-1)(p-2)(p-3)! \equiv 2(p-3)! \pmod{p}$.

2.12

In 1732 Euler wrote: "I derived [certain] results from the elegant theorem, of whose truth I am certain, although I have no proof: $a^n - b^n$ is divisible by the prime $n+1$ if neither a nor b is." Prove this theorem, using Fermat's Theorem.

Since $n+1 \nmid a$ and $n+1 \nmid b$, $(a, n+1) = 1$ and $(b, n+1) = 1$. We can thus use Fermat's Theorem to get $a^n \equiv 1 \pmod{n+1}$ and $b^n \equiv 1 \pmod{n+1}$. Subtracting these two congruences, have $a^n - b^n \equiv 0 \pmod{n+1}$, or, equivalently, $n+1 \mid a^n - b^n$.

2.13

Note that

$$\begin{aligned} 6! &\equiv -1 \pmod 7, \\ 5!1! &\equiv 1 \pmod 7, \\ 4!2! &\equiv -1 \pmod 7, \\ 3!3! &\equiv 1 \pmod 7. \end{aligned}$$

Try the same sort of calculation $\pmod{11}$.

$10! \equiv -1 \pmod{11}$ by Wilson's theorem. For the rest:

$$\begin{aligned} 9!1! &\equiv 1 \pmod{11}, \\ 8!2! &\equiv -1 \pmod{11}, \\ 7!3! &\equiv 1 \pmod{11}, \\ 6!4! &\equiv -1 \pmod{11}, \\ 5!5! &\equiv 1 \pmod{11}. \end{aligned}$$

2.14

Guess a theorem from the data of Problem 13, and prove it.

If p is prime, for $k \in [2, p-1]$, $(p-k)!(k-1)! \equiv -1^k \pmod p$.
$(p-1)! = (p-1) * (p-2) ... * (p-(k-1)) * (p-k)!$. From the product up to the $(p-k)!$ term we can cancel all factors of p, leaving us with $-1 * -2 * ... * -(k-1) = -1^{k-1} * (k-1)!$. So, we know that $(p-1)! \equiv -1^{k-1} * (k-1)! \equiv -1 \pmod p$. Multiplying both sides by the -1^{k-1} term, have $(p-k)!(k-1)! \equiv -1^k \pmod p$.

2.15

Suppose that p is an odd prime.
(a) Show that

$$1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1} \equiv -1 \pmod p$$

(b) Show that

$$1^p + 2^p + ... + (p-1)^p \equiv 0 \pmod p$$

(a) By Fermat's theorem, we have $a^{p-1} \equiv 1 \pmod p$ if $(a,p) = 1$. All $a \in [1, p-1]$ will have $(a,p) = 1$. So, the equation is equivalent to $1 + 1 + ... + 1 = p - 1 \equiv -1 \pmod p$.
(b) Fermat's Theorem can alternatively be stated $a^p \equiv a \pmod p$. So, our equation becomes $1 + 2 + ... + (p-1)$. Notice that this can be rearranged into $p/2$ pairs of a, $p-a$ so that the as cancel out, leaving only terms of p. So the sum must be $\equiv 0 \pmod p$.

2.16

Show that the converse of Fermat's Theorem is false. [Broad hint: consider $2^{340} \pmod{341}$.]

Write $341 = 11 * 31$ and find the residual of 2^{340} for both factors.

$$2^4 \equiv 5 \pmod{11}$$
$$2^8 \equiv 3 \pmod{11}$$
$$2^{16} \equiv 9 \pmod{11}$$
$$2^{32} \equiv 4 \pmod{11}$$
$$2^{64} \equiv 5 \pmod{11}$$
$$2^{128} \equiv 3 \pmod{11}$$
$$2^{256} \equiv 9 \pmod{11}$$
$$2^{340} = 2^{256+64+16+4} \equiv 1 \pmod{11}$$
$$2^5 \equiv 1 \pmod{31}$$
$$2^{340} \equiv 1 \pmod{31}$$

So, 2^{340} can be written as $(11 * 31)t + 1$, implying $2^{340} \equiv 1 \pmod{341}$ with 341 composite.

2.17

Show that for any two different primes p, q,
(a) $pq|(a^{p+q} - a^{p+1} - a^{q+1} + a^2)$ for all a.
(b) $pq|(a^{pq} - a^p - a^q + a)$ for all a.

(a) Write $a^{p+q} - a^{p+1} - a^{q+1} + a^2 = (a^p - a)(a^q - a)$. Note that each of these terms can be written $a(a^{x-1} - 1)$. Since the x in both is prime, by Fermat's Theorem $x|a^{x-1} - 1$. In other words, $p|(a^p - a)$ and $q|(a^q - a)$, so pq divides the whole thing.
(b) Fermat's Theorem can be stated $a^p \equiv a \pmod{p}$. So, $(a^q)^p \equiv a^q \pmod{p}$, and $a^{pq} - a^p \equiv a^q - a \pmod{p}$. Likewise, $a^{pq} - a^q \equiv a^p - a \pmod{q}$. So, subtracting the residue in either equation yields $a^{pq} - a^p - a^q + a$, which is divisible by both p and q.

2.18

Show that if p is an odd prime, then $2p|(2^{2p-1} - 2)$.

Can write $2^{2p-1} - 2 = 2(2^{2p-2} - 1) = 2(2^{p-1} - 1)(2^{p-1} + 1)$. We want to show that $p|(2^{p-1} - 1)(2^{p-1} + 1)$. Since $(p, 2) = 1$, we can use Fermat's Theorem to show that $p|(2^{p-1} - 1)$, so $2p|(2^{2p-1} - 2)$.

2.19

For what n is it true that

$$p|(1 + n + n^2 + ... + n^{p-2}) \ ?$$

If $p|n$ then we would need $p|1$ for the above to hold, so that is not a viable condition. The geometric series can be written $\frac{n^{p-1}-1}{n-1}$. As long as $(p, n) = 1$, we know by Fermat's Theorem that $p|(n^{p-1} - 1)$. We're not sure whether p divides the whole fraction if the bottom fraction is divisble by p. So, we should also exclude $n \equiv 1 \pmod{p}$ from viable n.

2.20

Show that every odd prime except 5 divides some number of the form 111...11 (k digits, all ones).

In the previous exercise, we showed $p|(1 + n + n^2 + ... + n^{p-2})$ if $n \not\equiv 0$ or $1 \pmod{p}$. Observe that numbers of the form 111...1 can be written as such a geometric series when $n = 10$. Since p is a prime other than 2 and 5, $10 \not\equiv 0 \pmod{p}$. For $p = 3$, have $3|111$. For $p = 7$, we know $10 \equiv 3 \pmod{7}$, so $\not\equiv 1$. All other primes are > 10, and thus be $\equiv 10 \pmod{p}$, so $\not\equiv 1$.