Number Theory Homework.

1. The Theorems of Fermat, Euler, and Wilson.

1.1. Fermat’s Theorem. The following is a special case of a result we have seen earlier, but as it will come up several times in this section, repeat it here.

**Proposition 1.** Let \( p \) be a prime and let \( a \) be an integer such that \( p \nmid a \). Then

\[
ax \equiv ay \pmod{p} \implies x \equiv y.
\]

**Proof.** If \( ax \equiv ay \pmod{p} \), then \( p \mid a(y - x) \). As \( p \) is prime this implies \( p \mid a \) or \( p \mid (y - x) \). But \( \nmid a \) and therefore \( p \mid (y - x) \) which implies \( x \equiv y \pmod{p} \). \( \square \)

**Proposition 2.** If \( p \) is prime, then \( p \nmid (p - 1)! \).

**Problem 1.** Prove this. \( \square \)

**Problem 2.** It is important that \( p \) is prime in the last result. Give an example where \( n \) is positive and composite and \( n \mid (n - 1)! \). More generally show that if \( n \geq 6 \) and \( n \) is composite, then \( n \mid (n - 1)! \). \( \square \)

The following is another result we have seen before.

**Proposition 3.** If \( p \) is prime and \( p \nmid a \), then after maybe reordering, the list of residue classes of

\[
a, 2a, 3a, \ldots, (p - 1)a
\]

is the same as the list of residue classes of

\[
1, 2, 3, \ldots, (p - 1).
\]

More explicitly we can reorder the set \( \{1, 2, 3, \ldots, (p - 1)\} \) as \( r_1, r_2, r_3, \ldots, r_{p-1} \) in such a way that

\[
a \equiv r_1 \pmod{p}, \quad 2a \equiv r_2 \pmod{p}, \quad \ldots \quad (p-1)a \equiv r_{p-1} \pmod{p}.
\]

**Proof.** Let \( 1 \leq j \leq (p - 1) \). Then \( p \nmid j \) and by assumption \( p \nmid a \). Therefore \( p \nmid ja \). Using the division to divide \( p \) into \( ja \) we get

\[
ja = q_jp + r_j \quad \text{where} \quad 1 \leq r_j \leq (p - 1).
\]

(The reason that \( r_j \neq 0 \) is that \( p \) does not divide \( ja \) and therefore the remainder is not 0.) Then

\[
ja \equiv r_j \pmod{p}
\]

If \( r_i = r_j \), then \( ia \equiv r_i = r_j \equiv ja \pmod{p} \). That is \( a_j \equiv ai \pmod{p} \). By Proposition 1 this implies \( i \equiv j \pmod{p} \). But \( 1 \leq i, j \leq (p - 1) \) and therefore \( i \equiv j \pmod{p} \) implies \( i = j \). Thus \( r_i = r_j \) implies \( i = j \). This implies that \( r_1, r_2, \ldots, r_{p-1} \) is a list of the \( (p - 1) \) distinct elements of \( \{1, 2, \ldots, (p - 1)\} \) a set of size \( (p - 1) \). Therefore the set \( r_1, r_2, \ldots, r_{p-1} \) is a list of the elements
of the set \( \{1, 2, \ldots, (p - 1)\} \) where each element appears exactly once in the list.

Let us look at an example related to these ideas. Let \( p = 11 \) and \( a = 4 \). Then Proposition 3 gives that

\[
1 \cdot 4, \ 2 \cdot 4, \ 3 \cdot 4, \ 4 \cdot 4, \ 5 \cdot 4, \ 6 \cdot 4, \ 7 \cdot 4, \ 8 \cdot 4, \ 9 \cdot 4, \ 10 \cdot 4
\]

are congruent mod 11 to the elements of the set \( \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \) in some order. And we can be specific

\[
1 \cdot 4 \equiv 4, \ 2 \cdot 4 \equiv 8, \ 3 \cdot 4 \equiv 1, \ 4 \cdot 4 \equiv 5, \ 5 \cdot 4 \equiv 9, \ 6 \cdot 4 \equiv 2, \ 7 \cdot 4 \equiv 6, \ 8 \cdot 4 \equiv 10, \ 9 \cdot 4 \equiv 3, \ 10 \cdot 4 \equiv 7,
\]

where all the congruences are mod 11. Now someone clever, mostly likely Fermat or Euler, had the idea of multiplying these all together to get

\[
(1 \cdot 4)(2 \cdot 4)(3 \cdot 4)(4 \cdot 4)(5 \cdot 4)(6 \cdot 4)(7 \cdot 4)(8 \cdot 4)(9 \cdot 4)(10 \cdot 4)
\]

\[
\equiv 4 \cdot 8 \cdot 1 \cdot 5 \cdot 9 \cdot 2 \cdot 6 \cdot 10 \cdot 3 \cdot 7 \mod 11
\]

By changing the order in the product we see

\[
4 \cdot 8 \cdot 1 \cdot 5 \cdot 9 \cdot 2 \cdot 6 \cdot 10 \cdot 3 \cdot 7 = 10!
\]

Also

\[
(1 \cdot 4)(2 \cdot 4)(3 \cdot 4)(4 \cdot 4)(5 \cdot 4)(6 \cdot 4)(7 \cdot 4)(8 \cdot 4)(9 \cdot 4)(10 \cdot 4) = 10! 4^{10}
\]

Combining these gives

\[
10! 4^{10} \equiv 10! \mod 11.
\]

But 11 \( \nmid \) 10! and therefore by Proposition 1 we can cancel the 10! to conclude

\[
4^{10} \equiv 1 \mod 11.
\]

There was nothing special about the prime 11 or the number 4 in this. Let us do another example, this time with \( p = 7 \) and \( a \) any integer with 7 \( \nmid \) a. Then by Proposition 3 the numbers

\[
a, \ 2a, \ 3a, \ 4a, \ 5a, \ 6a
\]

are \( \equiv \mod 7 \) to the numbers

\[
1, \ 2, \ 3, \ 4, \ 5, \ 6
\]

in some order. As the order of numbers in a product does not matter we thus have

\[
(a)(2a)(3a)(4a)(5a)(6a) \equiv (1)(2)(3)(4)(5)(6) \mod 7
\]

which implies

\[
6! a^6 \equiv 6! \mod 7.
\]

As 7 \( \nmid \) 6! we can cancel the 6! to get

\[
a^6 \equiv 1 \mod 7
\]

for all integers a such that 7 \( \nmid \) a.

At this point you may have already conjectured the following:
Theorem 4 (Fermat’s little Theorem). Let \( p \) be a prime and \( a \) an integer with \( p \nmid a \). Then
\[
a^{p-1} \equiv 1 \pmod{p}.
\]

Problem 3. Prove this. Hint: Here is an argument motivated by the examples above. Let \( r_1, r_2, \ldots, r_{p-1} \) be as in Proposition 3. In particular this means that \( r_1, r_2, \ldots, r_{p-1} \) a listing of the set \{1, 2, \ldots, (p-1)\} and
\[
a \equiv r_1 \pmod{p}, \quad 2a \equiv r_2 \pmod{p}, \quad \ldots \quad (p-1)a \equiv r_{p-1} \pmod{p}.
\]
These can be multiplied to get
\[
a(2a)(3a) \cdots ((p-1)a) \equiv r_1r_2r_3 \cdots r_{p-1} \pmod{p}.
\]
(a) Explain why
\[
r_1r_2r_3 \cdots r_{p-1} = (p-1)!. \]
(b) Show
\[
a(2a)(3a) \cdots ((p-1)a) = (p-1)!a^{p-1}.
\]
(c) Put these pieces together to conclude
\[
(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}
\]
Now you should be able to use Propositions 1 and 2 to finish the proof. \( \square \)

Fermat’s theorem is often stated in a slightly different form:

Theorem 5 (Fermat’s little Theorem). If \( p \) is a prime, then for any integer \( a \)
\[
a^p \equiv a \pmod{p}.
\]

Problem 4. Prove this. Hint: We are trying to show \( a^p - a = a(a^{p-1} - 1) \equiv 0 \pmod{p} \). Now consider two cases \( p \mid a \) (so that \( a \equiv 0 \pmod{p} \)) and \( p \nmid a \) (where the first form of Fermat’s Theorem applies). \( \square \)

Example 6. What is the remainder when \( 16^{205} \) is divided by 23? From Fermat’s little theorem we know that
\[
16^{22} \equiv 1 \pmod{23}.
\]
If we divide 22 into 205 the result is
\[
205 = 9(22) + 7.
\]
Therefore
\[
16^{205} = 16^{9(22)+7} = (16^{22})^9 (16)^7 = (1)^9 (16)^7 = 16^7.
\]
Now
\[
16^2 = 256 \equiv 3 \pmod{23}, \quad 16^4 = (16^2)^2 \equiv 3^2 \equiv 9 \pmod{23}.
\]
Thus
\[
16^{205} \equiv 16^7 \equiv 16 \cdot 16^2 \cdot 16^4 \equiv 16 \cdot 3 \cdot 9 \equiv 16 \cdot 4 \equiv 18 \pmod{23}
\]
where at one step we used \( 3 \cdot 9 = 27 \equiv 4 \pmod{23} \). Thus the remainder when \( 16^{205} \) is divided by 23 is 18. \( \square \)
Problem 5. Compute the following: (a) The remainder when \(10^{45}\) is divided by 13. (b) The remainder when \(605^{67}\) is divided by 7 (for this you may want to start by noting \(605 \equiv 3 \mod 7\)). (c) The remainder when \(23^{307}\) is divided by 31. □

Example 7. Find the remainder when \(7^{23}\) is divided by 15. Here Fermat’s Theorem does not apply directly, but the Chinese Remainder Theorem can help us out. Noting \(15 = 3 \cdot 5\). Let us find the remainder when \(7^{23}\) is divided by 3. In this case this is almost too easy:
\[
7^{23} \equiv 1^{23} \equiv 1 \quad \mod 3.
\]
Now we have \(7^{23} \equiv 2^{23} \mod 5\) and by Fermat’s Theorem \(2^4 \equiv 1 \mod 5\). Thus
\[
7^{23} \equiv 2^{23} \equiv (2^4)^5(2^3) \equiv 8 \cdot 8 \equiv 3 \quad \mod 5.
\]
Therefore \(7^{23}\) is a solution to the Chinese Remainder Problem
\[
x \equiv 1 \mod 3
\]
\[
x \equiv 3 \mod 5.
\]
We solve this and find the least positive solution is \(x = 13\). The solution to this Chinese Remainder Problem is unique modulo the product \(3 \cdot 5 = 15\). Thus
\[
7^{23} \equiv 13 \mod 15
\]
and therefore the remainder when \(7^{23}\) is divided by 15 is 13. □

Problem 6. Use the method of the last example to find the remainder when \(9^{45}\) is divided by 21. □

Problem 7. Find the remainder when \(6^{273}\) is divided by \(5 \cdot 7 \cdot 11 = 385\) by finding the remainders when it is divided by 5, 7, and 11 and then using the Chinese Remainder Theorem. □

Here is a more interesting application of Fermat’s Theorem.

Proposition 8. Let \(p\) be a prime and \(a\) an integer with \(p \nmid a\). Then \(\hat{a} := a^{p-2}\) is an inverse of \(a\) modulo \(p\). That is
\[
\hat{a}a \equiv 1 \mod p.
\]

Problem 8. Prove this. Hint: \(\hat{a}a = a^{p-1}\). □

1.2. Binomial coefficients and another proof of Fermat’s Theorem.
To motivate this recall the binomial theorem for \(n = 3\):
\[
(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3.
\]
If we view this modulo 3 and use that \(3 \equiv 0 \mod 3\) we find
\[
(x + y)^3 \equiv x^3 + y^3 \mod 3
\]
holds for all integers \(x\) and \(y\). Now let \(a\) be an integer such that
\[
a^3 \equiv a \mod 3.
\]
Then
\[(a + 1)^3 \equiv a^3 + 1^3 \mod 3 \equiv a + 1 \mod 3\]
(Using \(a^3 \equiv a \mod 3\)).

Therefore we have that for any integer \(a\)
\[a^3 \equiv a \mod 3 \implies (a + 1)^3 \equiv (a + 1) \mod 3\]
and we have a “base case” of \(a = 0\):
\[0^3 \equiv 0 \mod 3.

Thus by induction we have that \(a^3 \equiv a \mod 3\) for all \(a \geq 0\). If \(a < 0\) then \(b = -a > 0\) and so \(b^3 \equiv b \mod 3\). Thus
\[a^3 \equiv (-b)^3 \equiv -b^3 \equiv -b \equiv a \mod 3\]
and it follows that \(a^3 \equiv a\) for all integers \(a\).

Next consider
\[(x + y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5.\]
The coefficients of all but the first and last term are divisible by 5 which implies
\[(x + y)^5 \equiv x^5 + y^5 \mod 5,
and therefore we can do similar inductive proof to show that \(a^5 \equiv a \mod 5\) for all \(a\).

As one more example
\[(x + y)^7 = x^7 + 7x^6y + 21x^5y^2 + 35x^4y^3 + 35x^3y^4 + 21x^2y^5 + 7xy^6 + y^7\]
and again all the coefficients other than the first and last are divisible by 7 leading to
\[(x + y)^7 \equiv x^7 + y^7 \mod 7\]
for all integers \(x\) and \(y\).

So what we would like to be true is

**Proposition 9.** Let \(p\) be a prime and \(1 \leq k \leq p - 1\). Then the binomial coefficient \(\binom{p}{k}\) is divisible by \(p\). That is
\[\binom{p}{k} \equiv 0 \mod p\quad\text{for}\quad 1 \leq k \leq p.

**Lemma 10.** If \(p\) is a prime and \(k < p\) then \(p \nmid k!\).

**Problem 9.** Prove this. *Hint:* Towards a contradiction assume that \(p \mid k! = 1 \cdot 2 \cdot 3 \cdots k\). Then, as \(p\) is prime, \(p\) must divide one of the factors in this product. □
Proof of Proposition 9. Let \( p \) be prime and \( 1 \leq k \leq (p - 1) \).

\[
\binom{p}{k} = \frac{p!}{k!(p-k)!}.
\]

This implies

\[
p! = k!(p-k)! \binom{p}{k}
\]

and in particular that \( p \) divides \( k!(p-k)! \binom{p}{k} \). As \( p \) is prime this implies

\[
p \mid k!, \quad p \mid (p-k)!, \quad \text{or} \quad p \mid \binom{p}{k}.
\]

But \( k < p \) so by that last lemma \( p \nmid k! \). As \( k \geq 1 \) we have \((p-k) < p\) so the last lemma again applies and \( p \nmid (n-k)! \). This only leaves \( p \mid \binom{p}{k} \). \( \square \)

Proposition 11. If \( p \) is prime then for any integers \( x \) and \( y \)

\[
(x + y)^p \equiv x^p + y^p \mod p.
\]

More generally for any integers \( x_1, x_2, \ldots, x_m \) the congruence

\[
(x_1 + x_2 + \cdots + x_m)^p = x_1^p + x_2^p + \cdots + x_m^p
\]

holds.

Problem 10. Prove this. Hint: To prove the first congruence start with

\[
(x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{n-k} y^k
\]

and use \( \binom{p}{k} \equiv 0 \mod p \) for \( k = 1, 2, \ldots, p-1 \) to see that when this is viewed \( \mod p \) all but the first and last terms vanish. The second congruence follows form the first one by an easy induction. \( \square \)

Problem 11. Use the last proposition to show for any prime for any prime \( p \)

\[
a^p \equiv a \mod p \quad \implies \quad (a + 1)^p \equiv (a + 1) \mod p
\]

and use this to give an induction proof of Fermat’s Theorem that \( a^p \equiv a \mod p \). Hint: This can be done along the lines of the proof we gave in the case of \( p = 3 \) above. \( \square \)

Problem 12. Here is yet another way to prove Fermat’s theorem. Let \( p \) be a prime. Then by Proposition 11 we have for any integers \( x_1, x_2, \ldots, x_n \) that

\[
(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \mod p.
\]

If \( a \) is a positive integer let \( n = a \) and \( x_1 = x_2 = \cdots = x_n = 1 \). Then this congruence becomes

\[
(1 + 1 + \cdots + 1)^p \equiv 1^p + 1^p + \cdots + 1^p \mod p
\]

and you should be able to reduce this to \( a^p \equiv a \mod p \). Now show it also holds for negative \( a \). \( \square \)
Problem 13. Show that the following identities do not hold.

\[(x + y)^4 \equiv x^4 + y^4 \pmod{4}\]
\[(x + y)^6 \equiv x^6 + y^6 \pmod{6}\]
\[(x + y)^8 \equiv x^8 + y^8 \pmod{8}\]
\[(x + y)^9 \equiv x^9 + y^9 \pmod{9}\]

Recreational Extra Credit Problem. Show that if \(n \geq 2\) is an integer such that

\[(x + y)^n \equiv x^n + y^n \pmod{n}\]

for all integers \(x\) and \(y\), then \(n\) is a prime number.

1.3. Euler’s Theorem. Euler’s theorem is a generalization of Fermat’s theorem to moduli that are not prime. It requires a few definitions to do this. Let