Theory of Numbers homework 6
Fermat’s little theorem, Wilson’s theorem
Due October 9th, 2018

Exercise 1. For every integer \( n \geq 0 \), show that 13 divides \( 11^{12n+6} + 1 \).

Solution. By Fermat’s little theorem, \( 11^{12} \equiv 1 \pmod{13} \). Thus, for every \( n \geq 0 \), \( 11^{12n} \equiv 1 \pmod{13} \). Now, we have \( 11 \equiv -2 \pmod{13} \), so \( 11^2 \equiv 4 \pmod{13} \), so \( 11^4 \equiv 3 \pmod{13} \), and, multiplying the last two congruences, \( 11^6 = 11^2 \times 11^4 \equiv 4 \times 3 \equiv -1 \pmod{13} \). Thus, we have \( 11^{12n+6} \equiv -1 \pmod{13} \), whence the result.

Exercise 2. 1. Show that if \( p \) is a prime, then
\[
1 + 2 + \ldots + (p-1) \equiv -1 \pmod{p}.
\]

Solution. By Fermat’s little theorem, each of the \( p-1 \) terms on the left-hand side is congruent to 1 modulo \( p \), so that the sum is congruent to \( p-1 \equiv -1 \pmod{p} \).

2. Show that if \( p \) is an odd prime, then
\[
1 + 2 + \ldots + (p-1) \equiv 0 \pmod{p}.
\]

Solution. By the corollary to Fermat’s little theorem, the left-hand side is congruent to \( 1 + 2 + \ldots + (p-1) \pmod{p} \). The well-known formula for the sum of the \( p-1 \) first integers tells us that this is congruent to \( \frac{p(p-1)}{2} \pmod{p} \). Since \( p \) is odd, \( p-1 \) is even, \( \frac{p-1}{2} \) is an integer. This means that \( \frac{p(p-1)}{2} \) is congruent to 0 modulo \( p \), which gives the result.

Exercise 3. Solve \( x^{21} \equiv 6 \pmod{7} \).

Solution. We know \( x^7 \equiv x \pmod{7} \) by Fermat’s little theorem (or, more precisely the corollary to it), so \( x^{21} \equiv x^3 \pmod{7} \). Thus, the initial congruence is equivalent to \( x^3 \equiv 6 \pmod{7} \). Now, it suffices to compute the cubes of 0, 1, 2, . . . , 6 modulo 7 to find all solutions:

\[
\begin{array}{cccccccc}
a & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
a^3 & 0 & 1 & 6 & 1 & 6 & 1 & 6 \\
\end{array}
\]

Thus, the solutions are exactly all the integers congruent to 3, 5 or 6 modulo 7.

Exercise 4. Using Fermat’s little theorem, find the units digit of \( 3^{111} \).

Solution. The units digit is detected using congruences modulo 10, but 10 is not a prime so we won’t be able to use Fermat’s little theorem modulo 10. Therefore, we are going to look modulo 5. By Fermat’s little theorem, \( 3^4 \equiv 1 \pmod{5} \). On the other hand, \( 111 = 4 \times 27 + 3 \), so that
\[
3^{111} = (3^4)^{27} \times 3^3 \equiv 3^3 \equiv 2 \pmod{5}.
\]

This means that the units digit is either 2 or 7. Moreover, \( 3^{111} \) is odd, so the units digit must be 7.

Exercise 5. For any integer \( a \), show that \( a^5 \) and \( a \) have the same units digit.

Solution. First of all, \( a^5 \) and \( a \) are either both odd or both even, so \( a^5 \equiv a \pmod{2} \). Moreover, by the corollary to Fermat’s little theorem, \( a^5 \equiv a \pmod{5} \), so 2 and 5 both divide \( a^5 - a \). By lemma 2.3.12 in the lecture notes, we have that 10 divides \( a^5 - a \), so \( a^5 \) and \( a \) have the same units digit.
Exercise 6. If \( p \) and \( q \) are distinct primes, prove

\[
p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.
\]

Solution. Since \( p, q \geq 2 \) are distinct primes, they are relatively prime, so by Fermat’s theorem, we have \( p^{q-1} + q^{p-1} \equiv p^{q-1} \equiv 1 \pmod{q} \) and \( p^{q-1} + q^{p-1} \equiv q^{p-1} \equiv 1 \pmod{p} \). This means that \( p^{q-1} + q^{p-1} - 1 \) is divisible by \( p \) and by \( q \). By lemma 2.3.12 in the lecture notes, we have that \( pq \) divides \( p^{q-1} + q^{p-1} - 1 \), whence the result.

Exercise 7. Find the remainder in the Euclidean division of \( 15! \) by \( 17 \).

Solution. By Wilson’s theorem, \( 16! \equiv -1 \pmod{17} \). On the other hand, note that \( 16! = 16 \times 15! \equiv -15! \pmod{17} \), so that we see that \( 15! \equiv 1 \pmod{17} \).

Exercise 8. Show that \( 18! \equiv -1 \pmod{437} \).

Solution. Note that \( 437 = 19 \times 23 \), and that 19 and 23 are both primes. Now, first of all, \( 18! \equiv -1 \pmod{19} \) by Wilson’s theorem. On the other hand, by Wilson’s theorem again, we have \( 22! \equiv -1 \pmod{23} \). Observe that moreover

\[
22! = 18! \times 19 \times 20 \times 21 \times 22 \equiv 18! \times (-4) \times (-3) \times (-2) \times (-1) \pmod{23}
\]
\[
\equiv 18! \times 24 \pmod{23}
\]
\[
\equiv 18! \pmod{23}.
\]

As a conclusion, we have \( 18! \equiv -1 \pmod{23} \). We have that both 19 and 23 divide \( 18! + 1 \), so by lemma 2.3.12 in the lecture notes, we may conclude that 437 divides \( 18! + 1 \), which gives the result.

Exercise 9. Let \( p \) be a prime congruent to 3 modulo 4.

1. Show that \( \left(\frac{p-1}{2}\right)! \) is congruent to 1 or \(-1\) modulo \( p \).

Solution. We proceed as in the proof of the theorem on the quadratic congruence \( x^2 \equiv -1 \) in the lectures (see Burton Theorem 5.5), except that now \( -(\frac{p-1}{2}) \) is equal to \(-1\), so that we get that \( -(\frac{p-1}{2})! \) satisfies the congruence \( x^2 \equiv 1 \pmod{p} \). Now, any solution of this congruence is congruent to 1 or \(-1\) modulo \( p \), because \( x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p} \) implies that \( x - 1 \equiv 0 \pmod{p} \) or \( x + 1 \equiv 0 \pmod{p} \).

2. Show that the product of all the even positive integers less than \( p \) is congruent to 1 or \(-1\) modulo \( p \).

Solution. The said integers are exactly the integers of the form \( 2k \) with \( 2 \leq 2k \leq p - 1 \), so \( 1 \leq k \leq \frac{p-1}{2} \). Their product is therefore equal to

\[
2^{p-1} \left(\frac{p-1}{2}\right)!.
\]

By the previous question and proposition 5.6.4 in the lecture notes, we have the result.