Math 362 Assignment 5

Due: Friday, November 22

- Answer all questions. Each question is worth 5 marks. Full marks will be awarded only for answers that are both mathematically correct and coherently written.
- Please consider the markers and write neatly and legibly! I have instructed the markers to ignore work they cannot read. (And I won't read it, either.)

1. Suppose p is prime, $a \in \Phi(p)$ and $a^{(p-1)/2} \equiv -1 \pmod{p}$. Does it follow that a is a primitive root of p? If so, prove it. If not, give a counterexample.

   Answer

   It does not follow. Note that $8 \in \Phi(13)$. By Theorem 12.3, 2 is a primitive root of 13, hence $\operatorname{ord}_{13} 2 = 12$. Therefore, $(2^3)^4 \equiv 2^{12} \equiv 1 \pmod{13}$, from which we deduce that $\operatorname{ord} 8_{13} \leq 4$. However, $8^6 \equiv 8^{(13-1)/2} \equiv -1 \pmod{13}$.

2. Prove that for any integer $n \geq 3$, the integer 2^n has no primitive roots. Proceed as follows:

   (a) Prove by induction on n that if a is an odd integer, then

   $$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

   for all $n \geq 3$.

   (b) Deduce the required result.

   Answer

   (a) If $n = 3$, the congruence is $a^2 \equiv 1 \pmod{8}$. Since a is odd, the least residue of $a \pmod{8}$ is one of $1, 3, 5, 7$. Since $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}$, the statement is true for $n = 3$.

   Assume the statement to be true for $n = k$, that is, assume

   $$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

   This means that

   $$a^{2^{k-2}} = 2^k r + 1,$$

   for some integer r.

   Now, squaring both sides, we get

   $$\begin{aligned}(a^{2^{k-2}})^2 &= (2^k r + 1)^2, \quad \text{or} \\ a^{2^{k-1}} &= 2^{2k} r^2 + 2^{k+1} r + 1 = 1 + 2^{k+1}(r + 2^{k-1} r^2).\end{aligned}$$

But this implies that

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

Therefore the statement is also true for $n = k+1$, and the result follows by the Principle of Induction.

(b) Let $a \in \Phi(2^n)$, $n \geq 3$. Then 2^n is even, so a is odd, since $(a, 2^n) = 1$. Moreover, $\phi(2^n) = 2^n \cdot \frac{1}{2} = 2^{n-1}$. However, by (a),

$$a^{2^{n-2}} \equiv 1 \pmod{2^n}$$

and therefore $\operatorname{ord}_{2^n} a \leq 2^{n-2} < 2^{n-1} = \phi(2^n)$. This shows that a is not a primitive root of 2^n, from which it follows that 2^n has no primitive roots.

3. Use Legendre symbols to determine whether the congruence $x^2 \equiv 91 \pmod{103}$ has solutions.

Answer

Since $91 = 7 \times 13$, we have

$$\begin{aligned}
(91/103) &= (7/103)(13/103) & \\
&= -(103/7)(103/13) & \text{by the QRT; } 7 \equiv 103 \equiv 3 \pmod{4},\ 13 \equiv 1 \pmod{4} \\
&= -(5/7)(12/13) & 103 \equiv 5 \pmod{7},\ 103 \equiv 12 \pmod{13} \\
&= -(7/5)(4/13)(3/13) & \text{by the QRT; } 5 \equiv 1 \pmod{4} \\
&= -(2/5)(3/13) & 4 = 2^2, \text{ so } (4/13) = 1;\ 7 \equiv 2 \pmod{5} \\
&= (3/13) & (2/5) = -1 \text{ by Theorem 11.6} \\
&= (13/3) & \text{by the QRT; } 13 \equiv 1 \pmod{4} \\
&= (1/3) = 1. &
\end{aligned}$$

Hence the congruence has solutions.

4. Use Legendre symbols to determine whether 7 is a primitive root of the prime 4583.

Answer

Since

$$\begin{aligned}
(7/4583) &= -(4583/7) & \text{by the QRT, because } 7 \equiv 4583 \equiv 3 \pmod{4} \\
&= -(5/7) & \text{by Thm 11.3 A} \\
&= -(7/5) & \text{by the QRT, because } 5 \equiv 1 \pmod{4} \\
&= -(2/5) & \text{by Thm 11.3 A} \\
&= 1 & \text{by Theorem 11.6.}
\end{aligned}$$

Therefore 7 is a quadratic residue of 4583. By Euler's Criterion, $7^{2291} \equiv 1 \pmod{4583}$. Hence $\operatorname{ord}_{4583} 7 \leq 2291 < 4582 = \phi(4583)$, which means that 7 is not a primitive root of 4583.

5. Find (i) the period and (ii) the length of the non-periodical part of the

   (a) decimal expansion of $\frac{45}{252}$

   (b) base 6 expansion of $\frac{45}{252}$

   without finding the expansion itself.

   Answer

   (a) Since $\frac{45}{252} = \frac{5}{28} = \frac{5}{2^2 7}$ in lowest form, the period of the expansion is $\operatorname{ord}_7 10$. As shown in Table 15.1, $\operatorname{ord}_7 10 = 6$. Hence the period of the expansion is 6. The length of the non-periodical part is 2, because the highest power of 2 in 28 is 2 and the highest power of 5 is 0.

   (b) Since $\frac{45}{252} = \frac{5}{2^2 7}$ in lowest form, the period of the expansion is $\operatorname{ord}_7 6 = 2$. The length of the non-periodical part is 2, for the same reason as above.

6. Find the decimal expansion of $\frac{5}{28}$.

   Answer

   Note that $\frac{5}{2^2 7} = \frac{5^3}{10^2 7}$. Since $10^6 - 1 = 999\ 999 = 142\,857 \cdot 7$,

$$\frac{1}{7} = \frac{142\,857}{10^6 - 1} = \frac{142\,857}{10^6(1 - \frac{1}{10^6})}.$$

   Therefore

$$\begin{aligned}\frac{5}{2^2 7} &= \frac{5^3}{10^2}\frac{1}{7} = \frac{1}{10^2}\left(\frac{5^3 \cdot 142\ 857}{10^6 - 1}\right) = \frac{1}{10^2}\frac{17\,857\,125}{999999} = \frac{1}{10^2}\left(17 + \frac{857\,142}{10^6 - 1}\right)\\ &= \frac{1}{10^2}\left(17 + \frac{857\,142}{10^6(1 - 10^{-6}}\right) = \frac{1}{10^2}\left(17 + \frac{857\,142}{10^6}(1 + 10^{-6} + 10^{-12} + \cdots\right)\\ &= \frac{17}{10^2} + \left(\frac{857\,142}{10^8}(1 + 10^{-6} + 10^{-12} + \cdots\right) = 0.17\overline{857\,142}.\end{aligned}$$

7. Let $p = 24k - 1$, $k \in \mathbb{N}$, be a prime number. Explain why neither 2 nor 3 is a primitive root of p.

   Answer

   Since $p \equiv -1 \pmod{24}$ and $3, 4, 8$ and 12 are divisors of 24, we have that $p \equiv -1 \equiv 2 \pmod{3}$, $p \equiv -1 \equiv 3 \pmod{4}$, $p \equiv -1 \pmod{8}$ and $p \equiv -1 \pmod{12}$.

   By Theorem 11.6 and Euler's criterion,

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

We use Legendre symbols to find $(3/p)$:

$$\begin{aligned}(3/p) &= -(p/3) \quad \text{(by the QRT and because } p \equiv 3 \pmod{4}) \\ &= -(2/3) \quad \text{(because } p \equiv 2 \pmod{3}) \\ &= (-1)(-1) = 1 \quad \text{(Theorem 11.6).}\end{aligned}$$

By Euler's criterion,

$$1 = (3/p) \equiv 3^{(p-1)/2} \pmod{p}.$$

Hence $\operatorname{ord}_p 2 < \phi(p)$ and $\operatorname{ord}_p 3 < \phi(p)$, so 2 and 3 are not primitive roots of p.

8. [4] (Bonus question; no help given) Find an integer n such that the last ten digits of 7^n are 0000000001.

Answer

Consider 10^{10}. Its only prime divisors are 2 and 5, hence $(7, 10^{10}) = 1$.

By Euler's generalization of Fermat's little theorem, $7^{\phi(10^{10})} \equiv 1 \pmod{10^{10}}$. Since $\phi(10^{10}) = 10^{10}(\frac{1}{2})(\frac{4}{5}) = 2^{11}5^9$, we know that $7^{2^{11}5^9} \equiv 1 \, (\mathrm{mod}\, 10^{10})$. Therefore the last 10 digits of $7^{2^{11}5^9}$ are 0000000001.

Hence let $n = 2^{11}5^9$. (It is not necessarily the smallest integer with the desired property.)