

Assignment 1

1. For each prime p less than 30 find an integer a such that $\text{ord}_p(a) = p - 1$.

Solution.

Recall that $\text{ord}_p(a)$ (the order of a mod p) is the least integer $k > 0$ such that $a^k \equiv 1 \pmod{p}$. Note that if $a \equiv b \pmod{p}$ then $a^k \equiv b^k \pmod{p}$ for all k ; so a and b will have the same order mod p . Hence we can restrict our attention to residues (i.e. natural numbers less than p). And we can ignore 0 since it is never true that $0^k \equiv 1 \pmod{p}$ for $k > 0$.

The primes are 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29. Let us do $p = 29$ first, to demonstrate the method – which is just trial and error.

We will check if 2 has order 28, if it does not we will try 3, if that also fails we will try 5, and so on. Note that if $29 \nmid a$ then $\text{ord}_{29}(a)$ has to be a divisor of 28 (by Fermat's Little Theorem); so if we can show that none of a, a^2, a^4, a^7 and a^{14} are congruent to 1 mod 29 then it will follow that $\text{ord}_{29}(a) = 28$.

Trying $a = 2$, we compute the mod 29 residues of powers of 2 by multiplying the residues of lower powers of 2 and reducing mod 29. We find $2^1 \equiv 2, 2^2 \equiv 4, 2^4 \equiv 4^2 \equiv 16$, and then

$$2^7 = 2 \times 2^4 \times 2^2 \equiv (2 \times 16) \times 4 \equiv 32 \times 4 \equiv 3 \times 4 \equiv 12.$$

Finally, $2^{14} = (2^7)^2 \equiv 12^2 = 144 \equiv -1$. Since 2, $2^2, 2^4, 2^7$ and 2^{14} are not congruent to 1, it follows that $\text{ord}_{29}(2) = 28$.

You were only required to find one a such that $\text{ord}_{29}(a) = 28$, but since there are several different integers a with this property, there are several correct answers. In fact, if a is any number such that $\text{ord}_{29}(a) = 28$ then $\text{ord}_{29}(a^k) = 28$ whenever $\text{gcd}(a, 28) = 1$. So in fact there are $\phi(28)$ different correct answers less than 28. (They are actually 2, 8, 3, 19, 18, 14, 27, 21, 26, 10, 11 and 15.)

Now consider $p = 23$. The possible values for $\text{ord}_{23}(a)$ are 1, 2, 11 and 22. Obviously $2^1 = 2$ and $2^2 = 4$ are not congruent to 1 mod 23. We see that $2^4 \equiv -7$ and so $2^8 \equiv 7^2 \equiv 3$. Now

$$2^{11} = 2^8 \times 2^2 \times 2 \equiv 3 \times 4 \times 2 \equiv 1.$$

So $\text{ord}_{23}(2) = 11$. Bad luck, we will have to try another value for a ! Maybe 3 will do.

Clearly $3^1 = 3$ and $3^2 = 9$ are not congruent to 1 mod 23. We see that $3^4 \equiv -11$ and so $2^8 \equiv 121 \equiv 6$. Now

$$3^{11} = 3^8 \times 3^2 \times 3 \equiv 6 \times 9 \times 3 \equiv 1.$$

Oh well, try 5.

Obviously $5^1 = 5$ and $5^2 = 2$ are not congruent to 1 mod 23. We see that $5^4 \equiv 2^2 \equiv 4$ and so $5^8 \equiv 4^2 \equiv -7$. Now

$$5^{11} = 5^8 \times 5^2 \times 5 \equiv -7 \times 2 \times 5 \equiv -1.$$

We are in business. Since $5^1, 5^2, 5^{11}$ are not congruent to 1, we must have $\text{ord}_{23}(5) = 22$. So $a = 5$ is a correct answer. Other the correct answers less than 23 are the mod 23 residues of 5^k where $\text{gcd}(k, 22) = 1$. These are 5, 10, 20, 17, 11, 21, 19, 15, 7, 14.

Now consider $p = 19$. and try 2 first. We find that $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^6 = 64 \equiv 7$ and $2^9 = 2^3 \times 2^6 \equiv 8 \equiv 18$. So $\text{ord}_{19}(2)$ is not 1, 2, 3, 6 or 9; so it must be 18. The full list of correct answers less than 18 is 2, 13, 14, 15, 3, 10 (residues of 2^k where $\text{gcd}(k, 18) = 1$).

Now $p = 17$. Clearly $2^4 = 16 \equiv -1$, giving $2^8 \equiv 1$. So 2 is no good; let's try 3. We have $3^1 = 3, 3^2 = 9 \equiv -8, 3^4 \equiv 8^2 \equiv -4$ and so $3^8 \equiv 16$. So 3 does not have order 1, 2, 4 or 8; so it must have order 16. The full list of correct answers less than 17 is 3, 10, 5, 11, 14, 7, 12, 6 (the residues of 3^k for k odd).

Now $p = 13$. We have $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 \equiv 3, 2^6 \equiv 2^4 \times 2^2 \equiv 12$. So 2 does not have order 1, 2, 3, 4 or 6, and hence must have order 12. The full list of correct answers less than 13 is 2, $6 \equiv 2^5, 11 \equiv 2^7$ and $7 \equiv 2^{11}$.

Now $p = 11$. We have $2^1 = 2, 2^2 = 4, 2^5 = 32 \equiv 10$. So $\text{ord}_{11}(2)$ is not 1, 2 or 5; so it must be 10. The full list of correct answers is 2, $8 \equiv 2^3, 7 \equiv 2^7$ and $6 \equiv 2^9$.

Now $p = 7$. Clearly $2^3 \equiv 1$; so 2 is no good. But $3^1 = 3, 3^2 \equiv 2$ and $3^3 \equiv 6$ are all not congruent to 1; so $\text{ord}_7(3)$ must be 6. The full list of correct answers less than 7 is obtained by finding the residue of 3^k for every k coprime to 6. This just means 3^1 and 3^5 . Now $3^5 \equiv 5 \pmod{7}$; so the full list is just 3 and 5.

Now $p = 5$. There will be $\phi(4) = 2$ correct answers less than 5, and obviously 1 and 4 are no good (since $4 \equiv -1$ gives $4^2 \equiv 1$). This only leaves 2 and 3, and it is readily checked that indeed both are O.K.

Now $p = 3$. Since $a = 1$ is obviously no good, 2 had better work. It does: $2^1 \not\equiv 1$; so $\text{ord}_3(2)$ must be 2.

Finally, when $p = 2$ we want an a with order 1. Since 1 has no proper divisors, 1 is in fact the only possible order. And there is only one nonzero residue mod 2, namely 1. The correct answer is 1.

2. Find the general solution of the simultaneous congruences

$$\begin{aligned} 7x &\equiv 1 \pmod{13}, \\ 6x &\equiv 3 \pmod{15}, \\ 4x &\equiv 5 \pmod{11}. \end{aligned}$$

Solution.

We can write the condition $7x \equiv 1 \pmod{13}$ as $7x \equiv 14 \pmod{13}$, and then coprime cancellation gives $x \equiv 2 \pmod{13}$. So

$$x = 13k + 2 \quad (1)$$

for some integer k . The congruence $6x \equiv 3 \pmod{15}$ is equivalent to $2x \equiv 1 \pmod{5}$; so (1) gives $26k + 4 \equiv 1 \pmod{5}$. Thus

$$k \equiv 26k \equiv -3 \equiv 2 \pmod{5}$$

so that $k = 5l + 2$ for some integer l . Putting this back in (1) gives

$$x = 65l + 28 \quad (2)$$

for some integer l . Now putting this into $4x \equiv 5 \pmod{11}$ gives

$$5 \equiv 4x \equiv 4(65l + 28) \equiv 4(-l + 6) \equiv -4l + 24 \equiv -4l + 2 \pmod{11},$$

and so $4l \equiv -3 \equiv 8 \pmod{11}$. Thus $l \equiv 2 \pmod{11}$, and writing $l = 11m + 2$ we deduce from (2) that $x = 715m + 158$ for some integer m .

It is important to note that all of our steps above were two way implications: so not only is it true that every x satisfying the original three congruences can be written in the form $715m + 158$ for some integer m , it is also true that every number of this form is a solution.

The solution can also be written as $x \equiv 158 \pmod{715}$.

3. (MATH2068)

- (i) Let n be a positive integer and p a prime divisor of $n^2 - 1$. Show that either $n \equiv 1 \pmod{p}$ or $n \equiv -1 \pmod{p}$.
- (ii) By Fermat's Little Theorem $2^{46} \equiv 1 \pmod{47}$. Use Part (i) to deduce that $2^{23} \equiv \pm 1 \pmod{47}$.
- (iii) Since $2 \equiv 7^2 \pmod{47}$ it follows that $2^{23} \equiv 7^{46} \pmod{47}$. Use this and Fermat's Little Theorem to eliminate one of the possibilities in Part (ii), and hence show that $2^{23} - 1$ is not prime.

Solution.

- (i) We proved in lectures that if p is prime and $p|ab$ then $p|a$ or $p|b$. If we assume that p is prime and $p|(n^2 - 1)$ then we have that $p|(n - 1)(n + 1)$,

and so $p|(n - 1)$ or $p|(n + 1)$. Now by definition $n \equiv 1 \pmod{p}$ means exactly that $n - 1$ is a multiple of p , while $n \equiv -1 \pmod{p}$ means exactly that $n - (-1)$ is a multiple of p . So $p|(n - 1)$ or $p|(n + 1)$ gives $n \equiv 1$ or $n \equiv -1$, as required.

- (ii) Put $n = 2^{23}$. Then $n^2 = 2^{46} \equiv 1 \pmod{47}$, by Fermat's Little Theorem (as we were told). So $47|n^2 - 1$, and by Part (i) it follows that $n \equiv 1$ or $n \equiv -1 \pmod{47}$, as required.
- (iii) Indeed it is true that $7^2 = 49$ is congruent to 2 modulo 47. So it follows that $7^{46} = (7^2)^{23} \equiv 2^{23} \pmod{47}$. But applying Fermat's Little Theorem again tells us that $7^{46} \equiv 1 \pmod{47}$ (since 47 is prime and 7 is not a multiple of 47). So $2^{23} \equiv 1 \pmod{47}$, which means that $47|(2^{23} - 1)$. So $2^{23} - 1$ is not prime.

(Recall that numbers of the form $2^n - 1$ with n prime are called Mersenne numbers, and recall that $2^n - 1$ can never be prime unless n is prime. So the only numbers of the form $2^n - 1$ that can be prime are the Mersenne numbers. Unfortunately, it is not the case that all Mersenne numbers are prime; indeed, the above question shows that the Mersenne number $2^{23} - 1$ is not prime. In fact there is one smaller Mersenne number that is not prime, namely $2^{11} - 1$: one can show by an argument very similar to the one above that $23|(2^{11} - 1)$.)

3. (MATH2988)

Let p be a prime and let m be the Mersenne number $2^p - 1$. Let the sequences s_i and t_i be defined as in Question 6 of Tutorial 5, and suppose that $s_{\frac{1}{4}(m+1)} \equiv 0 \pmod{m}$. [Note: See the MATH2988 web page for some relevant extra reading.]

- (i) By imitating the method used in Exercise 4 of Tutorial 3, or otherwise, prove that if q is a prime then q must be a divisor of at least one element of the set $\{t_i \mid 1 \leq i \leq q + 1\}$
- (ii) Let q be a prime and let k be the least positive integer such that $q|t_k$. Using Exercise 6 (i) of Tutorial 5, show that if $n \in \mathbb{N}$ then $q|t_n$ if and only if $k|n$. (We call k the *entry point* for q in the sequence (t_n) .)
- (iii) Show that if q is any prime divisor of m then its entry point in (t_n) is $\frac{1}{2}(m + 1) = 2^{p-1}$. (Hint: The entry point divides 2^{p-1} but not 2^{p-2} .)
- (iv) Deduce from Parts (ii) and (iii) that the only possible prime divisor of m is m itself.

Solution.

- (i) Suppose, for a contradiction, that q is not a divisor of any of the numbers t_i for $1 \leq i \leq q + 1$. For each $i \in \{1, 2, \dots, q\}$ define u_i to be the least natural number satisfying $u_i t_i \equiv t_{i+1} \pmod{q}$. (We know that $x t_i \equiv t_{i+1} \pmod{q}$ has a solution x since $\gcd(t_i, q) = 1$.) Since $(u_i - q)t_i \equiv u_i t_i$ it follows that $u_i - q$ must be negative; so $0 \leq u_i < q$. Observe also that $u_1 \equiv 4 \pmod{q}$, since $t_1 = 1$ and

$t_2 = 4$. Now for $i > 1$ the recurrence relation for the t_i gives $4t_i - t_{i-1} = 4t_{i+1}$; so for $1 < i \leq q$ we have

$$4t_i - t_{i-1} \equiv u_i t_i \pmod{q},$$

and thus $t_{i-1} \equiv (4 - u_i)t_i \pmod{q}$. This shows that $u_i \neq 4$, when $1 < i \leq q$, since $q \nmid t_{i-1}$. Moreover,

$$t_{i-1} \equiv (4 - u_i)t_i \equiv (4 - u_i)(u_{i-1}t_{i-1}) \pmod{q},$$

and by cancelling t_{i-1} we deduce that $4 - u_i$ is the inverse of u_{i-1} modulo q . So the value of u_{i-1} determines the value of u_i , and the value of u_i determines the value of u_{i-1} .

We have seen above that $4 = u_1 \notin \{u_i \mid 1 < i \leq q\}$. We now use induction on j to show that $u_j \notin \{u_i \mid j \leq i \leq q\}$, for all j from 1 to q ; this will show that the numbers u_1, u_2, \dots, u_q are pairwise distinct. Since the case $j = 1$ has been done, we may assume that $j > 1$, and the inductive hypothesis tells us that $u_{j-1} \notin \{u_i \mid j-1 \leq i \leq q\}$. So if $j < i \leq q$ then $u_{j-1} \not\equiv u_{i-1} \pmod{q}$. Recall that $4 - u_j$ and $4 - u_i$ are the inverses of u_{j-1} and $u_{i-1} \pmod{q}$; so if u_j were equal to u_i we would have

$$u_{j-1} \equiv u_{j-1}(4 - u_i)u_{i-1} = u_{j-1}(4 - u_j)u_{i-1} \equiv u_{i-1} \pmod{q}$$

contrary to what was shown above. So $u_j \notin \{u_i \mid j \leq i \leq q\}$, as required to complete the induction.

Since u_1, u_2, \dots, u_q are pairwise distinct and lie in the set $\{0, 1, \dots, q-1\}$, it follows from the pigeonhole principle that one of them is zero. So there is an i such that $1 \leq i \leq q$ and $u_i = 0$. But this gives $t_{i+1} \equiv u_i t_i \equiv 0 \pmod{q}$, contradicting our initial assumption that none of the numbers t_1, t_2, \dots, t_q are divisible by q , and thereby completing the proof of Part (i).

(ii) Obviously $k > 1$, since $q \nmid 1 = t_1$. Now $t_k \equiv 0 \pmod{q}$ and $t_{k-1} \not\equiv 0 \pmod{q}$, by the definition of k , and it follows that $t_{k+1} = 4t_k - t_{k-1} \equiv -t_{k-1} \not\equiv 0 \pmod{q}$. So $q \nmid t_{k+1}$, and since q is a prime it follows, for all integers M , that $q \mid Mt_{k+1}$ if and only if $q \mid M$. Since Exercise 6 (i) of Tutorial 5 tells us that $t_{k+i} \equiv t_i t_{k+1} \pmod{q}$ for all $i \in \mathbb{N}$, we deduce that $q \mid t_{k+i}$ if and only if $q \mid t_i$. It follows by induction that if $g \in \mathbb{N}$ is arbitrary then $q \mid t_{gk+i}$ if and only if $q \mid t_i$. (The case $g = 0$ is trivial, and the inductive step follows since $q \mid t_{gk+i} = t_{k+(g-1)k+i}$ if and only if $q \mid t_{(g-1)k+i}$.)

Now given $n \in \mathbb{N}$, choose g and i such that $n = gk + i$ and $0 \leq i < k$. (The Division Algorithm guarantees that we can do this, since k is a positive integer.) If $i = 0$ then $t_i = 0$ and $q \mid t_i$, but if $i \neq 0$ then $q \nmid t_i$, since $i < k$. So $q \mid t_i$ if and only if $i = 0$; that is, $q \mid t_i$ if and only if $k \mid n$. But $q \mid t_{gk+i}$ if and only if $q \mid t_i$; so $q \mid t_n = t_{gk+i}$ if and only if $k \mid n$, as required.

(iii) We are given that $m \mid s_{\frac{1}{4}(m+1)}$, and so $q \mid s_{\frac{1}{4}(m+1)}$. By Exercise 6 (ii) of Tutorial 5 it follows that $t_{\frac{1}{2}(m+1)} = s_{\frac{1}{4}(m+1)} t_{\frac{1}{4}(m+1)}$, which therefore must also be a multiple of q . Since $q \mid t_n$ if and only if $k \mid n$, we deduce that $k \mid \frac{1}{2}(m+1)$. That is, $k \mid 2^{p-1}$. We conclude that k must be equal to 2^i for some i such that $0 \leq i \leq p-1$.

Let $k = 2^i$, and suppose, for a contradiction, that $i \leq p-2$. Then $k \mid 2^{p-2}$, and so $q \mid t_{2^{p-2}}$. That is, $q \mid t_{\frac{1}{4}(m+1)}$. But by Exercise 6 (iii) of Tutorial 5 we have that $s_{\frac{1}{4}(m+1)}^2 - 12t_{\frac{1}{4}(m+1)}^2 = 4$. Since both terms on the left are multiples of q it follows that $q \mid 4$, which is obviously impossible since q is a prime divisor of m , which is odd. So i must be $p-1$; that is, the entry point of q in the sequence (t_i) is 2^{p-1} .

(iv) As in Part (iii), let q be a divisor of m and let k be the entry point of q in the sequence (t_i) . We know from Part (i) that $k \leq q+1$. That is, $q \geq k-1$. So Part (iii) tells us that $q \geq 2^{p-1} - 1$. If $q \neq m$ then since q is a divisor of m we must have $q \leq \frac{m}{2} = \frac{1}{2}(2^p - 1) = 2^{p-1} - \frac{1}{2}$. Since q is an integer we conclude that $q = 2^{p-1} - 1$, and $m = 2q + 1$, contradicting the fact that $q \mid m$. So $q = m$, and m is prime, as required.