

### Math 445 Homework 3 Solutions

11. When applying the Pollard  $\rho$  method, starting from  $a_1$ , suppose we find that  $a_1, \dots, a_{17}$  are all distinct, mod  $n$ , but then  $a_{18} \equiv a_{11}$ . Find the smallest  $k$  for which  $a_{2k} \equiv a_k$ .

Since  $a_{18} \equiv a_{11}$ ,  $a_{19} = f(a_{18}) \equiv f(a_{11}) = a_{12}$ , and, in fact,  $a_{k+7} \equiv a_k$  for every  $k \geq 7$ . (This can be formally proved by induction.) This, in turn, implies (formally, again, by induction on  $m$ ) that  $a_{k+7m} \equiv a_k$  for all  $m \geq 1$  and  $k \geq 11$ . In fact, these are the *only* pairs of terms of the sequence  $\{a_n\}_{n=1}^{\infty}$  that are mutually congruent - after  $a_{11}$ , the terms keep going around in a circle with a period of 7. So, to solve the problem, we wish to have  $2k = k + 7m$  for some  $m \geq 1$  and  $k \geq 11$ , i.e.,  $k = 7m$  for some  $m \geq 1$  and  $k \geq 11$ . The first  $m$  which works is therefore  $m = 2$ , with  $k = 14$ ;  $a_{28} \equiv a_{14}$ , and no smaller  $k$  works.

12. Show that if  $n = pq$  is a product of distinct primes and  $de \equiv 1 \pmod{(p-1)(q-1)}$ , then  $A^{de} \equiv A \pmod{n}$ .

We'll show that  $A^{de} \equiv A \pmod{p}$  and  $A^{de} \equiv A \pmod{q}$ , i.e.,  $p$  and  $q$  both divide  $A^{de} - A$ . Then since  $p$  and  $q$  are distinct primes,  $(p, q) = 1$ , and so  $n = pq | A^{de} - A$ .

By hypothesis,  $de - 1 = k(p-1)(q-1)$ , so  $de = 1 + k(p-1)(q-1)$ . Given  $A$ , one of three things is true: (1)  $(A, p) = (A, q) = 1$ , (2) exactly one of  $p, q$  divides  $A$ , WOLOG  $p | A$  (since there is no distinction between them) and  $(A, q) = 1$ , or (3)  $p, q | A$ , so  $n = pq | A$ .

In case (1), Fermat's Little Theorem tells us that  $A^{p-1} \equiv 1 \pmod{p}$  and  $A^{q-1} \equiv 1 \pmod{q}$ , so  $A^{de} = (A^{p-1})^{k(q-1)} A \equiv 1^{k(q-1)} A \equiv A \pmod{p}$  and  $A^{de} = (A^{q-1})^{k(p-1)} A \equiv 1^{k(p-1)} A \equiv A \pmod{q}$  as desired. In case (2),  $A \equiv 0 \pmod{p}$ , so  $A^{de} \equiv 0^{de} \equiv 0 \equiv A \pmod{p}$ , while, as in (1),  $A^{de} \equiv A \pmod{q}$ . Finally, in case (3),  $A \equiv 0 \pmod{p}$  and  $A \equiv 0 \pmod{q}$ , so  $A^{de} \equiv 0^{de} \equiv 0 \equiv A \pmod{p}$  and the same for  $q$ . So in all cases,  $A^{de} \equiv A \pmod{p}$  and  $A^{de} \equiv A \pmod{q}$ , so  $A^{de} \equiv A \pmod{n}$ .

13. If  $p^2 | n$  for some  $p \geq 2$ , then there are  $a \not\equiv b \pmod{n}$  for which  $a^k \equiv b^k \pmod{n}$  for every  $k \geq 2$ .

Since  $p^2 | n$ , we have  $n = p^2 s$  for some integer  $s$ . Set  $a = 0$  and  $b = ps$ ; then  $a \not\equiv b \pmod{n}$ , since  $n \nmid px = b - a = ps$ . (This is where  $p \geq 2$  is used;  $n > ps$  so  $n$  cannot divide  $ps$ .) But  $b^2 = p^2 x^2 = nx \equiv 0 = a^2$ , and, in fact,  $n = p^2 x | b^k$  for every  $k \geq 2$ , since  $b^k = p^k x^k = (p^2 x)(p^{k-2} x^{k-1})$ , so  $a^k = 0 \equiv b^k$  for all  $k \geq 2$ .

14. If  $n | m$ , and  $(10, m) = 1$ , then the period of the decimal expansion of  $1/n$  divides the period of the decimal expansion of  $1/m$ .

Translating this into the language of orders, if  $n | m$  and  $(10, m) = 1$ , then we wish to show that  $\text{ord}_n(10) | \text{ord}_m(10)$ . Setting  $s = \text{ord}_m(10)$ , it is enough to show that  $10^s \equiv 1 \pmod{n}$ , since we know that  $\text{ord}_n(10)$  divides any such exponent. But by definition,  $10^s \equiv 1 \pmod{m}$ , so  $m | 10^s - 1$ , so  $10^s - 1 = mx$  for some  $x$ . But since  $n | m$ ,  $m = ny$  for some  $y$ , so  $10^s - 1 = mx = (ny)x = n(xy)$ , so  $n | 10^s - 1$ , so  $10^s \equiv 1 \pmod{n}$ , as desired.

15. For every  $n \geq 2$ ,  $\text{ord}_{3^n}(10) = 3^{n-2}$  .

We show first that for every  $n \geq 2$ ,  $10^{3^{n-2}} = 1 + k3^n$  for some  $k$  with  $(k, 3) = 1$ . We proceed by induction. For  $n = 2$ ,  $10^{3^{2-2}} = 10^{3^0} = 10^1 = 10 = 1 + 1 \cdot 3^2$  , so  $k = 1$  and  $(1, 3) = 1$  . Now suppose that  $10^{3^{n-2}} = 1 + k3^n$  for some  $k$  with  $(k, 3) = 1$ . Then

$$\begin{aligned} 10^{3^{(n+1)-2}} &= 10^{3^{n-2} \cdot 3} = (10^{3^{n-2}})^3 = (1 + k3^n)^3 \\ &= 1 + 3(1)^2(k3^n) + 3(1)(k3^n)^2 + (k3^n)^3 \\ &= 1 + k3^{n+1} + k^2 3^{2n+1} + k^3 3^{3n} \\ &= 1 + (k + k^2 3^n + k^3 3^{2n-1}) 3^{n+1} \end{aligned}$$

with  $k + k^2 3^n + k^3 3^{2n-1} \equiv k + k^2(0) + k^3(0) \equiv k \pmod{3}$  (since  $n, 2n - 1 \geq 1$ ) . So  $(k + k^2 3^n + k^3 3^{2n-1}, 3) = (k, 3) = 1$  , so  $10^{3^{(n+1)-2}} = 1 + K3^{n+1}$  with  $(K, 3) = 1$ , as desired. So by induction, for  $n \geq 2$  ,  $10^{3^{n-2}} = 1 + k3^n$  for some  $k$  with  $(k, 3) = 1$ .

Since  $10^{3^{n-2}} = 1 + k3^n$ ,  $10^{3^{n-2}} \equiv 1 \pmod{3^n}$ , so  $\text{ord}_{3^n}(10) | 3^{n-2}$ . So either  $\text{ord}_{3^n}(10) = 3^{n-2}$  or  $\text{ord}_{3^n}(10) = 3^m$  for some  $m < n - 2$ . But we know from above that  $10^{3^m} - 1 = k3^{m+2}$  for some  $k$  with  $(k, 3) = 1$ . So if  $\text{ord}_{3^n}(10) = 3^m$ , then  $3^n | 10^{3^m} - 1$ , so  $10^{3^m} - 1 = s3^n$  for some  $s$ . But then  $k3^{m+2} = s3^n$ , so cancelling powers of 3,  $k = s3^{n-(m+2)} = s3^{(n-2)-m} = s3^r$  for some  $r \geq 1$ . So  $3|k$ , so  $(k, 3) = 3$ , a contradiction. So  $\text{ord}_{3^n}(10) = 3^{n-2}$  , as desired.