

Solutions/ Hints to homework 4

January 28, 2008

section 2.1

28. True. We have that $(r, s)|r$ and $r|(a - c)$, hence $(r, s)|(a - c)$. Similarly $(r, s)|(b - c)$. Therefore $(r, s)|(a - b)$, since $a - b = (a - c) - (b - c)$.

29. Quick calculation shows that a has to be congruent to 4 or 6 modulo 10. If $a = 4 + 10k$, then $a^2 - 16 = 80k + 100k^2$ is congruent to 0 mod 20. Similarly in the other case.

30. We need to prove that $30|a^5 - a$. We have $a^5 - a = a(a^4 - 1) = a(a + 1)(a - 1)(a^2 + 1)$. Note that $3|a(a + 1)(a - 1)$ and $2|a(a + 1)$. Now we only need to show that $5|a(a + 1)(a - 1)(a^2 + 1)$. If 5 divides $(a - 1)$ or a or $(a + 1)$ we are done. Assume then that 5 does not divide $a(a + 1)(a - 1)$. Then a has to be congruent to 2 or 3 modulo 5. In either case $5|(a^2 + 1)$.

section 2.2

11. Assume that there is an ordering of Z_n . Then either $0 < 1$ or $1 < 0$. If for example $1 < 0$, then adding 1 $n - 1$ times to both sides gives $n < n - 1 < \dots < 1$, i.e. $0 < 1$ which contradicts the assumption $1 < 0$. Similarly in the other case.

section 2.3

7. a) $x=16$ b) $x=14$ c) $x=21$ d) $x=20$ e) $x=6$ f) no solutions

Let's just explain the last one. We use Thm. 2.11. We have that $(a, n) = (15, 63) = 3$ and 3 does not divide $b=5$.

8. Let's follow the hint: assume that $ar = b$ in Z_n . Then $ar - b = kn$ for some integer k , or equivalently $b = ar - kn$. Since $d|a$ and $d|n$ we get that $d|b$.

9. Since $d = (a, n)$ we can write d as a linear combination of a and n with integer

coefficients $d = au + nv$. Since $d|b$ (given), $d|a$ and $d|n$ (because $d = (a, n)$) we can find integers b_1, a_1, n_1 such that $b = b_1d, a = a_1d, n = n_1d$.

Let $k \in \{0, 1, \dots, (d-1)\}$. We will show that $ub_1 + kn_1$ is a solution to the equation $ax = b$ in Z_n . We have (the calculations below are in Z):

$$a(ub_1 + kn_1) = (au)b_1 + an_1k = (d - nv)b_1 + (a_1d)n_1k = db_1 - nvb_1 + a_1n = b + nq,$$

where $q = -vb_1 + a_1$. Therefore $a(ub_1 + kn_1) = b$ in Z_n .

10. We need to show two things:

- (1) the solutions we produced in ex. 9 are all distinct
- (2) the list of solutions is complete (i.e. those are all solutions).

Proof of (1): Suppose that in Z_n we have $ub_1 + kn_1 = ub_1 + ln_1$ where $k, l \in \{0, \dots, (d-1)\}$. This implies $(k-l)n_1 = 0$ in Z_n , or equivalently $n|(k-l)n_1$. Note also that $-d < k-l < d$ and hence $-n < (k-l)n_1 < n$. Therefore since $n|(k-l)n_1$ we must have that $(k-l)n_1 = 0$ in Z , i.e. $k = l$.

Proof of (2): Let r be a solution of the equation $ax = b$ in Z_n , i.e. $ar = b$ in Z_n . We also know that $aub_1 = b$. Combining these two together we get $a(r - ub_1) = 0$ in Z_n , or equivalently $n|a(r - ub_1)$. Therefore we have $n_1d = n = a(r - ub_1)k = a_1d(r - ub_1)k$ for some integer k , or equivalently $n_1 = a_1(r - ub_1)k$. This means that $n_1|a_1(r - ub_1)$. Since $(n_1, a_1) = 1$ we conclude that $n_1|(r - ub_1)$, i.e. $r - ub_1 = kn_1$ for some integer k . Therefore $r = ub_1 + kn_1$, and since we $r = ub_1 + kn_1 \in Z_n$, we can assume WLOG that $0 \leq k \leq d-1$.