

18.781: Ideas for solutions to problem set 4

2.3 (3) Use the algorithm which is the proof of the Chinese remainder theorem. So set $m_1 = 4$, $m_2 = 3$, and $m_3 = 7$ so $m = 84$. Then the b_i are defined by the condition that $b_i(m/m_i) \equiv 1 \pmod{m_i}$. In this case, $b_1 = 1$, $b_2 = 1$, and $b_3 = 3$ works. And now the CRT tells us that

$$1 \cdot 21 \cdot 1 + 1 \cdot 28 \cdot 0 + 3 \cdot 12 \cdot 5 = 21 + 180 = 201$$

works, and that every other solution is $201 + 84k$, where k runs over all integers.

2.3 (12) Since $7200 = 2 \cdot 3600$ and 3600 is divisible by 2 , a number n is relatively prime to 3600 if and only if $(n, 7200) = 1$. Thus the answer to the question is $\phi(7200)$. Now $7200 = 2^5 \cdot 3^2 \cdot 5^2$ so by theorem 2.19 the answer is

$$(2^5 - 2^4)(3^2 - 3)(5^2 - 5) = (16)(6)(20) = 1920.$$

2.3 (15) By theorem 2.20, the number of solutions to the given congruence is equal to the product of the number of solutions to the congruences

$$X^3 + 4X + 8 \equiv 0 \pmod{3}, \quad X^3 + 4X + 8 \equiv 0 \pmod{5}.$$

Plugging in $0, 1$ and 2 for X in the first congruence we see that the first congruence has 1 solutions ($X = 2$), and plugging $0, 1, 2, 3, 4$ into the second equation we see that it has no solutions, and hence the equation has no solutions modulo 15 .

2.3 (21) If there is a solution, call it a , to the system, then $a \equiv a_r \pmod{p^{\alpha_r}}$. Since $\alpha_r \geq \alpha_i$ for all i , theorem 2.1 part (5) shows that $a \equiv a_r \pmod{p^{\alpha_i}}$ for all i , and hence $a_r \equiv a_i \pmod{p^{\alpha_i}}$ for all i .

Conversely, if $a_r \equiv a_i \pmod{p^{\alpha_i}}$ for all i , then $X = a_r$ is a solution to the system.

2.3 (44) Write $m = \prod_i p_i^{\alpha_i}$. By theorem 2.3 part (3) it suffices to show that a^m is congruent to $a^{m-\phi(m)}$ modulo $p_i^{\alpha_i}$ for each i . So pick some i , and write $m = p_i^{\alpha_i} m'$, with $(m', p_i) = 1$. Then by theorem 2.19, $\phi(m) = (p^{\alpha_i} - p^{\alpha_i-1})\phi(m')$.

Now consider two cases. If $(a, p_i) = 1$, then

$$a^{\phi(p_i^{\alpha_i})} = a^{(p^{\alpha_i} - p^{\alpha_i-1})} \equiv 1 \pmod{p_i^{\alpha_i}},$$

so

$$a^{m-\phi(m)} \equiv a^{m-\phi(m)} \cdot (a^{(p^{\alpha_i} - p^{\alpha_i-1})})^{m'} \equiv a^m \pmod{p_i^{\alpha_i}}$$

and so the result holds in this case.

The second case is if $p_i | a$. In this case, we claim that both numbers are congruent to 0 modulo $p_i^{\alpha_i}$. Write $a = p_i a'$ for some a' , and note that both m and $\phi(m) = (p^{\alpha_i} - p^{\alpha_i-1})\phi(m')$ are divisible by $p_i^{\alpha_i-1}$. Therefore, on both sides of the congruence we have factors of $p_i^{\alpha_i-1}$. Since $p_i^{\alpha_i-1} \geq \alpha_i$, this implies that both sides are congruent to zero.

2.3 (45) Write $m = \prod_{i=1}^r p_i^{\alpha_i}$ in its prime factorization. We claim that the answer is 2^r . To see this, note that by theorem 2.20, it suffices to show that the answer to the question is 2 when $m = p^\alpha$ is a power of a prime.

Now when $m = p^\alpha$ is a power of a prime, what we are asking for are numbers x so that

$$x(x-1) \equiv 0 \pmod{p^\alpha}.$$

Now if p^α divides $x(x-1)$, then it must divide either x or $x-1$ for x and $x-1$ have no common factors (if $p|x$ and $p|x-1$ then $p|(x-(x-1))=1$). This shows that the only possible solutions in this case are $x=0$ or $x=1$. In particular, there are exactly 2 solutions.

2.4 (6) We show that 2047 is composite by applying the strong pseudo-prime test to the base 3. So write $2047-1=2046=2*1023$, and

$$1023 = \sum_{j=0}^9 2^j,$$

this follows for example from the fact that $2^{10}=1024$, or can be computed directly. We now compute $3^{1023} \pmod{2047}$. We have (everything modulo 2047)

$$3^4 = 81, 3^{2^3} = 420, 3^{2^4} = 358, 3^{2^5} = 1250, 3^{2^6} = 639, 3^{2^7} = 968, 3^{2^8} = 1545, 3^{2^9} = 223.$$

Assuming I did the calculation correctly we get

$$3^{1023} \equiv 1565 \pmod{2047}.$$

If 2047 were prime, this should be ± 1 , and hence 2047 must not be prime.

2.4 (16) To show that $d_n|d_{n+1}$, it suffices to show that d_n divides $2^{(n+1)!}-1$. Since $2^{n!} \equiv 1 \pmod{d_n}$, we see by raising both sides to the $(n+1)$ -st power that $2^{(n+1)!} \equiv 1 \pmod{d_n}$, and hence $d_n|2^{(n+1)!}-1$. Now if m has a prime factor p such that $(p-1)|n!$, then $p|d_n$. To see this, write $n!=(p-1)\ell$ for some ℓ and note that

$$2^{n!}-1 \equiv (2^{p-1})^\ell - 1 \equiv 1^\ell - 1 \equiv 0 \pmod{p},$$

by Fermat's theorem.

To find a divisor of 403, note that for $n=4$, we get that $13-1=12$ divides $n!$, and also divides 403. For $n=5$, we get that both $13-1$ and $31-1$ divide $5!$, and hence $d_5=403$.

2.5 (4) Since m is square-free, we can write $m=p_1 \cdots p_r$, with the p^i distinct primes. To verify that $a^{k\bar{k}} \equiv a \pmod{m}$ it suffices that $a^{k\bar{k}} \equiv a \pmod{p_i}$ for each i . Now if a is divisible by p_i , this is immediate. If $(a, p_i)=1$, then write $k\bar{k}=1+\ell\phi(m)=1+(p_i-1)\phi(m/p_i)\ell$, and observe that

$$a^{k\bar{k}} \equiv a \cdot (a^{p_i-1})^{\ell\phi(m/p_i)} \equiv a \pmod{p_i}$$

by Fermat's theorem.

2.5 (6) If p is a prime, then taking $m=p^2$, $a_1=0$, and $a_2=p$ we obtain the desired example.