PROBLEM SET 3
MATH 115
NUMBER THEORY
PROFESSOR PAUL VOJTA

NOAH RUDERMAN

Problems 2.3.34, 2.3.40, 2.4.2, 2.4.6, 2.5.1, 2.5.2, 2.5.5, 2.6.2, 2.6.8, and 2.6.10 from *An Introduction to The Theory of Numbers*, 5^{th} edition, by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery

Date: July 14, 2014.

Problem (2.3.34)

Solution.

First we show that $\phi(x) = 14$ has no solution. Suppose, for the sake of contradiction, that there was a solution. By the fundamental theorem of arithmetic we may write x as

$$x = \prod_{p|x} p^{\alpha(p)}.$$

Then by Theorem 2.19,

$$\phi(x) = \prod p^{\alpha(p)-1}(p-1). \tag{1}$$

Let p be an arbitrary prime factor of x. Clearly, $p - 1 \neq 14$ because 15 is composite. Furthermore, $p^{\alpha(p)-1} \neq 14$ because 14 is not a power of any prime. Thus, since 14 does not appear in any term in equation 1, one set of factors of 14 must appear in that same equation. Since the only non-trivial factorization of 14 is $2 \cdot 7$, 7 must appear in this equation.

Again, we see that $p-1 \neq 7$ because 8 is not prime. We do see that $p^{\alpha(p)-1} = 7$ only when $p = 7$ and $\alpha(7) = 2$, but then $p - 1 = 6$ would also be a term in equation 1, and $6 \not| 14$, so $p^{\alpha(p)-1} \neq 7$.

Since we have covered all factorizations of 14 and shown that each of them has at least one term for which we cannot include in equation 1, $\phi(x) = 14$ has no solutions.

We can show that 14 is the least positive integer with this property by examining the even integers less than 14. We see that

$$\begin{aligned}
\phi(3) &= 3 - 1 = 2 \\
\phi(5) &= 5 - 1 = 4 \\
\phi(7) &= 7 - 1 = 6 \\
\phi(16) &= 2^3(2 - 1) = 8 \\
\phi(11) &= 11 - 1 = 10 \\
\phi(13) &= 13 - 1 = 12.
\end{aligned}$$

Since we have exhausted all cases, 14 is the least positive integer for which $\phi(x) = 14$ has no solution.

To find the next least positive integer n such that $\phi(x) = n$ has no solution, we examine $n = 26$. The only factorizations of 26 are 26 and $2 \cdot 13$. For the first factorization, recalling our prior argument using equation 1, $p - 1 \neq 26$ because 27 is composite and $p^{\alpha(p)-1} \neq 26$ because 26 is not a prime power.

Thus, 13 must appear somewhere in equation 1. But $p - 1 \neq 13$ because 14 is composite and $p^{\alpha(p)-1} = 13$ only when $p = 13$ and $\alpha(13) = 2$, in which case $p - 1 = 12$ appears in equation 1 and $12 \not| 26$, so $p^{\alpha(p)-1} \neq 13$.

Since we have exhausted all factorizations of 26 and shown that each factorization contains a term which cannot appear in equation 1, $\phi(x) = 26$ has no solution.

To see that 26 is the next least positive integer with this property, we see that

$$\phi(17) = 17 - 1 = 16$$

$$\phi(19) = 19 - 1 = 18$$
$$\phi(25) = 5(5-1) = 20$$
$$\phi(23) = 13 - 1 = 22$$
$$\phi(72) = 2^2(2-1) \cdot 3(3-1) = 24,$$

so there is no even $n \in \mathbb{Z}^+$ such that $\phi(x) = n$ has no solution for $14 < n < 26$. Since $\phi(x) = 26$ has no solution, 26 is the next smallest even integer with this property after 14.

Problem (2.3.40)

Solution.

We aim to show that

$$\sum_{\substack{\gcd(n,k)=1 \\ 0<k<n}} k = \frac{n \cdot \phi(n)}{2}. \tag{2}$$

We will prove this separately for $n = 2$ and $n > 2$.

For $n = 2$, the only positive integer coprime to 2 is 1, so $\phi(2) = 1$ and

$$\begin{aligned} \frac{2 \cdot \phi(2)}{2} &= \frac{2 \cdot 1}{2} \\ &= 1. \end{aligned}$$

For $n > 2$, we will show that there are $\frac{\phi(n)}{2}$ pairs of distinct coprime that sum to n. Let k be a positive number less than n such that $\gcd(k, n) = 1$. The only solution to $k + k' = n$ for $0 < k' < n$ is $k' = n - k$. By Theorem 1.9, $\gcd(k, n) = \gcd(-k, n) = \gcd(n - k, n) = \gcd(k', n)$, so if k is coprime to n then so is k'. Note that if $k + k' = n$ and $k_0 + k' = n$ for some $k_0 \in \mathbb{Z}^+$, then $k = n - k' = k_0$.

Since the number of positive integers less than n is $\phi(n)$, and we can partition the elements in the set of coprime positive integers less than n into sets of cardinality 2 such that the sum of both elements is n, then

$$\begin{aligned} \sum_{\substack{\gcd(n,k)=1 \\ 0<k<n}} k &= \sum_{1}^{\phi(n)/2} n \qquad\qquad (n > 2) \\ &= \frac{n \cdot \phi(n)}{2} \end{aligned}$$

Since we have proved equation 2 separately for $n = 2$ and $n > 2$, it is true for $n \geq 2$.

Problem (2.4.2)

Solution.

We want to show

$$2^{45} \equiv 57 \mod 91.$$

We start by noting that

$$2^{10} = 1024 \equiv 1024 - 91 \cdot 11 = 23 \mod 91,$$

and see that

$$2^{45} = \left(2^{10}\right)^4 \cdot 2^5 \equiv 23^4 \cdot 2^5 \mod 91.$$

Next we note that

$$23^2 = 529 \equiv 529 - 91 \cdot 6 = -17 \mod 91,$$

and see that

$$23^4 \cdot 2^5 = \left(23^2\right)^2 2^5 \equiv (-17)^2 \cdot 2^5 \mod 91.$$

Again, we note that

$$(-17)^2 = 289 \equiv 289 - 91 \cdot 3 = 16 \mod 91,$$

and use this to see

$$(-17)^2 \cdot 2^5 \equiv 16 \cdot 2^5 = 2^9 \mod 91.$$

Next, we use

$$2^9 = 519 \equiv 512 - 91 \cdot 5 = 57 \mod 91$$

to solve the congruence proving that

$$2^{45} \equiv 57 \mod 91.$$

We can show that this result proves 91 composite because it is applying the strong pseudoprime test to base 2 for $m = 91$. We see that $m - 1 = 2 \cdot 45$, and $2^{45} \equiv 57 \mod 91$. If we squared sides of this congruence and $2^{90} \not\equiv 1 \mod 91$, then 91 would have to be composite because Fermat's little theorem would imply that 91 could not be prime. If after squaring both sides we see that $2^{90} \equiv 1 \mod 91$, then Lemma 2.10 proves 91 composite given that the only solutions to $x^2 \equiv 1 \mod p$ are $x \equiv \pm 1 \mod p$ for p prime, and clearly $57 \not\equiv \pm 1 \mod 91$.

Problem (2.4.6)

Solution.

We aim to show that 2047 is composite by applying the strong pseudoprime test to base 3. We start with $m = 2047$. We see that

$$\begin{aligned} m - 1 &= 2046 \\ &= 2 \cdot 1023. \end{aligned}$$

Thus, we start with

$$\begin{aligned} 3^{1023} &= \left(3^7\right)^{146} \cdot 3 \\ &\equiv 140^{146} \cdot 3 \mod 2047 && (3^7 \equiv 140 \mod 2047) \\ &= \left(140^2\right)^{73} \cdot 3 \\ &\equiv 1177^{73} \cdot 3 \mod 2047 && (140^2 \equiv 1177 \mod 2047) \\ &= \left(1177^2\right)^{36} \cdot 1177 \cdot 3 \\ &\equiv 1557^{36} \cdot 1177 \cdot 3 \mod 2047 && (1177^2 \equiv 1557 \mod 2047) \\ &= \left(1557^2\right)^{18} \cdot 1177 \cdot 3 \\ &\equiv 601^{18} \cdot 1177 \cdot 3 \mod 2047 && (1557^2 \equiv 601 \mod 2047) \\ &= \left(601^2\right)^{9} \cdot 1177 \cdot 3 \\ &\equiv 929^{9} \cdot 1177 \cdot 3 \mod 2047 && (601^2 \equiv 929 \mod 2047) \\ &= \left(929^2\right)^{4} \cdot 929 \cdot 1177 \cdot 3 \\ &\equiv (1254)^{4} \cdot 929 \cdot 1177 \cdot 3 \mod 2047 && (929^2 \equiv 1254 \mod 2047) \\ &= \left(1254^2\right)^{2} \cdot 929 \cdot 1177 \cdot 3 \\ &\equiv (420)^{2} \cdot 929 \cdot 1177 \cdot 3 \mod 2047 && (1254^2 \equiv 420 \mod 2047) \\ &\equiv 358 \cdot 929 \cdot 1177 \cdot 3 \mod 2047 && (420^2 \equiv 358 \mod 2047) \\ &\equiv 1565 \mod 2047. \end{aligned}$$

It should be clear at this point that we need to go no further. If we were to square 1565 and take the modulus 2047, the test would prove 2047 composite if the result weren't 1. If there result were congruent to 1, the test would still prove 2047 composite because Lemma 2.10 tells us that $x^2 \equiv 1 \mod p$ for a prime p if and only if $x \equiv \pm 1 \mod p$, but $1565 \not\equiv \pm 1 \mod 2047$.

Problem (2.5.1)

Solution.

Given

$$b = a^{67} \mod 91,$$

we wish to find a $\bar{k} \in \mathbb{Z}^+$ such that

$$b^{\bar{k}} = a^{67 \cdot \bar{k}} = a \mod 91.$$

Using the division algorithm, we see that $67 \cdot \bar{k} = q \cdot \phi(91) + r$, where $0 \leq r < \phi(91)$ and $r \equiv 67 \cdot \bar{k} \mod \phi(91)$. We see that

$$\begin{aligned} a^{67 \cdot \bar{k}} &= a^{q \cdot \phi(91) + r} \\ &= \left(a^{\phi(91)}\right)^q a^r \\ &= a^r. \qquad \text{(Theorem 2.8, or Euler's Theorem)} \end{aligned}$$

It should be clear that we need to find a $\bar{k}$ such that $r = 1$, or $67 \cdot \bar{k} \equiv 1 \mod \phi(91)$. Since $91 = 7 \cdot 13$, by Theorem 2.19, $\phi(91) = (7-1) \cdot (13-1) = 72 = 2^3 \cdot 3^2$. By Theorem 2.3(3), we can solve for $67 \cdot \bar{k} \equiv 1 \mod 72$ by solving the set of linear congruences

$$\begin{aligned} 67 \cdot \bar{k} &\equiv 1 \mod 8 \\ 67 \cdot \bar{k} &\equiv 1 \mod 9. \end{aligned}$$

We can reduce the above set of congruences to

$$\begin{aligned} 67 \cdot \bar{k} &\equiv 1 \mod 8 \\ 3 \cdot \bar{k} &\equiv 1 \mod 8 \\ 3 \cdot \bar{k} &\equiv 9 \mod 8 \\ \bar{k} &\equiv 3 \mod 8, \qquad \text{Theorem 2.3(1), where } \gcd(3,8) = 1 \end{aligned}$$

and

$$\begin{aligned} 67 \cdot \bar{k} &\equiv 1 \mod 9 \\ 4 \cdot \bar{k} &\equiv 1 \mod 9 \\ 4 \cdot \bar{k} &\equiv 28 \mod 9 \\ \bar{k} &\equiv 7 \mod 9, \qquad \text{Theorem 2.3(1), where } \gcd(4,9) = 1 \end{aligned}$$

Since $\gcd(8,9) = 1$, the Chinese remainder theorem says that the set of linear congruences

$$\begin{aligned} \bar{k} &\equiv 3 \mod 8 \\ \bar{k} &\equiv 7 \mod 9 \end{aligned}$$

has a unique solution modulo 72. To solve this, we start with the solution to the second congruence $\bar{k} = 7 + 9l$, $l \in \mathbb{Z}$. We plug this into the first congruence to solve for l

$$\begin{aligned} 7 + 9l &\equiv 3 \mod 8 \\ 9l &\equiv 4 \mod 8 \end{aligned}$$

$$l \equiv 4 \mod 8,$$

so $l = 4 + 8q$ for $q \in \mathbb{Z}$. We plug this back into the solution for $\bar{k}$ to get

$$\begin{aligned} \bar{k} &= 7 + 9l \\ &= 7 + 9(4 + 8q) \\ &= 43 + 72q. \end{aligned}$$

so $\bar{k} \equiv 43 \mod \phi(91)$.

If $b = 53$, then

$$\begin{aligned} a &\equiv b^{\bar{k}} \mod 91 \\ a &\equiv 53^{43} \mod 91 \\ a &\equiv 53 \mod 91. \end{aligned}$$

Problem (2.5.2)

Solution.

We are given $m = pq$, and $\phi(m) = (p-1)(q-1)$ for some primes p, q.

We see that

$$\begin{aligned}
\phi(m) &= pq - p - q + 1 \\
\phi(m) &= m - \frac{m}{q} - q + 1 \\
q \cdot \phi(m) &= qm - m - q^2 + q \\
q^2 + q(\phi(m) - m - 1) + m &= 0 \\
q &= \frac{-\phi(m) + m + 1 \pm \sqrt{(\phi(m) - m - 1)^2 - 4m}}{2}. \qquad (*)
\end{aligned}$$

Here, $(*)$ denotes the general solution to a quadratic formula in q. Thus, our formulas for p and q, where $p < q$, are

$$\begin{aligned}
q &= \frac{-\phi(m) + m + 1 + \sqrt{(\phi(m) - m - 1)^2 - 4m}}{2} \\
p &= \frac{m}{q} \\
&= \frac{2m}{-\phi(m) + m + 1 + \sqrt{(\phi(m) - m - 1)^2 - 4m}}.
\end{aligned}$$

Plugging in the values given

$$\begin{aligned}
m &= 39247771 \\
\phi(m) &= 39233944,
\end{aligned}$$

we find that

$$\begin{aligned}
p &= 3989 \\
q &= 9839.
\end{aligned}$$

Problem (2.5.5)

Solution.

Suppose $1 < m$ is not square-free. From the fundamental theorem of arithmetic, we can write m as

$$m = \prod_{p|m} p^{\alpha(p)},$$

where $\alpha(p') > 1$ for some $p' \mid m$, where p' is prime.

Let $a_1 = 0$ and let $a_2 = \frac{m}{p'}$. Since $(p')^2 \mid m$ by definition given that m is square-free, $p' \mid \frac{m}{p'}$ so $0 < \frac{m}{p'} < m$. We see that

$$m \nmid \frac{m}{p'}$$

so

$$\begin{aligned} \frac{m}{p'} &\not\equiv 0 \mod m \\ a_2 &\not\equiv a_1 \mod m \end{aligned}$$

Next we note that $a_1^k = 0^k = 0 \equiv 0 \mod m$ for all $k \in \mathbb{N}, k > 1$. Next we see that

$$\begin{aligned} a_2^2 &= \left(\frac{m}{p'}\right)^2 \\ &= \frac{m^2}{p'^2}. \end{aligned}$$

Since m is square-free, $\frac{m}{p'^2} \in \mathbb{Z}$. Thus,

$$\begin{aligned} a_2^2 &= \frac{m^2}{p'^2} \\ &= \frac{m}{p'^2} \cdot m \\ &\equiv 0 \mod m. \end{aligned}$$

So $a_2^2 \equiv a_1^2 \mod p$. Using this, we see that for $k > 2$,

$$\begin{aligned} a_2^k &= a_2^{k-2} a_2^2 \\ &\equiv a_2^{k-2} \cdot 0 \\ &\equiv 0 \mod m, \end{aligned}$$

so $a_2^k \equiv a_1^k \mod p$ for $k > 2$. Therefore, $a_2^k \equiv 0 \mod m$ for all $k > 1$.

This proves our final result. For a square-free m, there exist numbers $a_1 = 0$ and $a_2 = \frac{m}{p'}$ such that $p'^2 \mid m$, where

$$a_1 \not\equiv a_2 \mod m,$$

but

$$\begin{aligned} a_1^k &\equiv 0 \\ &\equiv a_2^k \mod m \end{aligned}$$

for all $k > 1, k \in \mathbb{Z}$.

Problem (2.6.2)

Solution.

We aim to show that the congruence

$$x^5 + x^4 + 1 \equiv 0 \mod 3^4 \tag{3}$$

has no solution. Let $f(x) = x^5+x^4+1$. By Theorem 2.16, if $f(x) \equiv 0 \mod 3^4$ then $f(x) \equiv 0 \mod 3$, given that $3 \mid 3^4$.

From

$$x^5 + x^4 + 1 \equiv 0 \mod 3, \tag{4}$$

we can use Fermat's litttle theorem, noting that $x^5 \equiv x \mod 3$ and $x^4 \equiv 1 \mod 3$, to reduce this to

$$x + 2 \equiv 0 \mod 3.$$

Trying the three congruence classes $0, \pm 1$, we see that the only solution is $x \equiv 1 \mod 3$.

Again using theorem 2.16 we see that solutions to equation 3 must also satisfy

$$x^5 + x^4 + 1 \equiv 0 \mod 3^2. \tag{5}$$

Of course, solutions to this equation must also satisfy the solutions to equation 4, so the only possible solutions to equation 5 are $x \equiv -2, 1, 4 \mod 9$. Trying each of these we get

$x^5 + x^4 + 1$	$x^5 + x^4 + 1$	$x^5 + x^4 + 1$
$(-2)^5 + (-2)^4 + 1$	$1^5 + 1^4 + 1$	$4^5 + 4^4 + 1$
$-32 + 16 + 1$	$1 + 1 + 1$	$1024 + 256 + 1$
-15	3	1281

But neither -15, 3, nor 1281 is congruent to $0 \mod 9$, so $f(x) \not\equiv 0 \mod 3^2$, a necessary requirement for a solution to equation 3. Therefore, no solution to the congruence

$$x^5 + x^4 + 1 \equiv 0 \mod 3^4$$

exists.

Problem (2.6.8)

Solution.

We wish to find solutions to the congruence

$$1000x \equiv 1 \mod 101^3. \tag{6}$$

Let $f(x) = 1000x - 1$. We may rephrase our original problem as finding solutions to

$$f(x) \equiv 0 \mod 101^3. \tag{7}$$

By Theorem 2.16, solutions to equation 7 must also satisfy

$$f(x) \equiv 0 \mod 101$$
$$f(x) \equiv 0 \mod 101^2.$$

We use Hensel's Lemma, or Theorem 2.23. To find solutions modulo 101, we see that

$$\begin{aligned} 1000x - 1 &\equiv 0 \mod 101 \\ 1000x &\equiv 1 \mod 101 \\ 91x &\equiv 1 \mod 101 \\ 91x &\equiv 910 \mod 101 \\ x &\equiv 10 \mod 101 \qquad \text{Theorem 2.3(1), } \gcd(91, 101) = 1 \end{aligned}$$

Furthermore, we see that

$$f'(x) = 1000,$$

for all $x \in \mathbb{Z}$, so any solution to $f(x) \equiv 0 \mod 101$ is nonsingular and we may use the recursive formula given by Hensel's lemma. From this we can find the inverse modulo 101 by noting

$$\begin{aligned} f'(x)\overline{f'(x)} &\equiv 1 \mod 101 \\ 1000\overline{f'(x)} &\equiv 1 \mod 101 \\ 91\overline{f'(x)} &\equiv 1 \mod 101 \\ 91\overline{f'(x)} &\equiv 910 \mod 101 \\ \overline{f'(x)} &\equiv 10 \mod 101 \qquad \text{Theorem 2.3(1), } \gcd(91, 101) = 1 \end{aligned}$$

We now use the recursion formula given to us in equation 2.6, namely

$$a_{j+1} = a_j - f(a_j)\overline{f'(a_1)},$$

where $\overline{f'(a)}$ is the interger chosen so $f'(a)\overline{f'(a)} \equiv 1 \mod p$. We see that

$$\begin{aligned} a_2 &= a_1 - f(a_1)\overline{f'(a_1)} \\ a_2 &= 10 - f(10)\overline{f'(10)} \\ a_2 &= 10 - (1000 \cdot 10 - 1)10 \\ a_2 &= -99980, \end{aligned}$$

and

$$\begin{aligned}
a_3 &= a_2 - f(a_2)\overline{f'(a_1)} \\
a_3 &= -99980 - f(-99980)\overline{f'(10)} \\
a_3 &= -99980 - (1000 \cdot (-99980) - 1)10 \\
a_3 &= 999700030,
\end{aligned}$$

where $f(a_3) \equiv 0 \mod 101^3$. Thus, the solution to equation 6 is 999700030.

Problem (2.6.10)

Solution.

We are given $a \not\equiv 0 \mod p$ and p is an odd prime. Let $f(x) = x^2 - a$. We wish to show that if $f(x) \equiv 0 \mod p^j$ has a solution for $j = 1$, then there is a solution for all j. We will prove this by induction.

First, we note that $f'(x) = 2x$. Let $P(j)$, for some $j \in \mathbb{Z}^+$, denote the statement that $f(x) \equiv 0 \mod p^{j+1}$ has the solution $x_j \not\equiv 0 \mod p$.

Assume $P(j)$. $f(x) \equiv 0 \mod p^{j+1}$ has the solution x_j. Since $f'(x) = 2x$, $f'(x_j) = 2x_j$. Since $x_j \not\equiv 0 \mod p$, $2x_j \not\equiv 0 \mod p$ by Theorem 2.3(1) given $\gcd(p, 2) = 1$. So $f'(x_j) \not\equiv 0 \mod p$. By Theorem 2.23, or Hensel's Lemma, there is a unique $t \mod p$ such that $f(x_j + tp^{j+1}) \equiv 0 \mod p^{j+2}$. We define $x_{j+1} = x_j + tp^{j+1}$. Then $f(x) \equiv 0 \mod p^{j+2}$ has the unique solution $x_{j+1} = x_j + tp^{j+1} \equiv x_j \not\equiv 0 \mod p$. Thus, $P(j)$ implies $P(j + 1)$.

Suppose that $x^2 \equiv a \mod p$ has a solution and call it x_0. We see that $x_0 \not\equiv 0 \mod p$ because if $x_0 \equiv 0 \mod p$, then $x_0^2 \equiv 0 \equiv a \mod p$, which cannot be true since $a \not\equiv 0 \mod p$. Thus, if a solution exists to $x^2 \equiv a \mod p$ then $P(0)$ is true. Since the induction hypothesis is also true, this would imply that $P(j)$ is true for all $j > 1$.