PROBLEM SET 4
MATH 115
NUMBER THEORY
PROFESSOR PAUL VOJTA

NOAH RUDERMAN

Problems 2.7.1a, 2.7.2, 2.7.6, 2.8.8a-f, 2.8.10, 2.8.11, 2.8.13, 2.8.16, 2.8.19, 2.8.21, 2.9.1a, 2.9.7, 3.1.7abcd, 3.1.11, and 3.1.12 from *An Introduction to The Theory of Numbers*, 5^{th} edition, by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery

Date: July 21, 2014.

Problem (2.7.1)

Solution.

a. We have

$$\begin{aligned} x^{11} + x^8 + 5 &\equiv 0 \mod 7 \\ x^6 \cdot x^5 + x^6 \cdot x^2 + 5 &\equiv 0 \mod 7 \\ x^5 + x^2 + 5 &\equiv 0 \mod 7, \qquad \text{(Fermat's little theorem)} \end{aligned}$$

which is an equivalent congruence of degree less than 6.

Problem (2.7.2)

Solution.

We reduce or original congruence as follows:

$$\begin{aligned} 2x^3 + 5x^2 + 6x + 1 &\equiv 0 \mod 7 \\ 4 \cdot (2x^3 + 5x^2 + 6x + 1) &\equiv 4 \cdot 0 \mod 7 \\ 8x^3 + 20x^2 + 24x + 4 &\equiv 0 \mod 7 \\ x^3 + 6x^2 + 3x + 4 &\equiv 0 \mod 7. \end{aligned}$$

Call $f(x) = x^3 + 6x^2 + 3x + 4$. Clearly, $f(x)$ has degree 3 and has the same solutions as our original congruence. To factor $x^7 - x = f(x)q(x) + p \cdot s(x)$, with deg $q(x) = 7 - 3 = 4$ and deg $s(x) < 3$ or $s(x)$ has no degree, we see that

$$\begin{aligned} (x^7 - x) - x^4 \cdot f(x) &= -6x^6 - 3x^5 - 4x^4 - x \\ (x^7 - x) - (x^4 - 6x^3) f(x) &= 33x^5 + 14x^4 + 24x^3 - x \\ (x^7 - x) - (x^4 - 6x^3 + 33x^2) f(x) &= -184x^4 - 75x^3 - 132x^2x^3 - x \\ (x^7 - x) - (x^4 - 6x^3 + 33x^2 - 184x) f(x) &= 1029x^3 + 420x^2 + 735x \\ (x^7 - x) - (x^4 - 6x^3 + 33x^2 - 184x + 1029) f(x) &= -5754x^2 - 2352x - 4116 \\ (x^7 - x) - (x^4 - 6x^3 + 33x^2 - 184x + 1029) f(x) &= 7(-822x^2 - 336x - 588). \end{aligned}$$

Setting

$$\begin{aligned} q(x) &= x^4 - 6x^3 + 33x^2 - 184x + 1029 \\ s(x) &= -822x^2 - 336x - 588, \end{aligned}$$

we see that

$$x^7 - x = f(x)q(x) + 7 \cdot s(x),$$

where deg $q(x) = 4$ with leading coefficient 1, and deg $s(x) = 2 < 3$.

By Theorem 2.29, $f(x)$ has exactly 3 solutions, and by extension so does the congruence

$$2x^3 + 5x^2 + 6x + 1 \equiv 0 \mod 7.$$

Problem (2.7.6)

Solution.

We aim to show that theorem 2.26, or

$$\textit{The congruence } f(x) \equiv 0 \mod m \textit{ of degree } n \textit{ has at most } n \textit{ solutions}$$

is false for a composite m.

Consider the congruence of degree 1, $f(x) = ax$, $a \in \mathbb{Z}$. By Theorem 2.17, $ax \equiv 0 \mod m$ has $\gcd(a, m)$ solutions. Since $f(x)$ has degree 1, $a_1 = a \not\equiv 0 \mod m$, so if m is composite, $\gcd(a, m)$ is not necessarily 1. In the case where $\gcd(a, m) > 1$, theorem 2.26 (with composite m) cannot hold because Theorem 2.17 implies that first-degree congruences can have more than one solution.

As an example, consider

$$2x \equiv 0 \mod 4.$$

Clearly, this is a first-degree congruence with 2 solutions: $x \equiv 0 \mod 4$ and $x \equiv 2 \mod 4$.

Problem (2.8.8)

Solution.

a. We have

$$x^{12} \equiv 16 \mod 17.$$

Clearly, $\gcd(16, 17) = 1$. We see that

$$\begin{aligned} 16^{\frac{17-1}{\gcd(12,17-1)}} &= 16^{\frac{16}{\gcd(12,16)}} \\ &= 16^{\frac{16}{4}} \\ &= 16^4 \\ &\equiv (-1)^4 \\ &= 1 \mod 17, \end{aligned}$$

so there are $\gcd(12, 16) = 4$ solutions.

b. We have

$$x^{48} \equiv 9 \mod 17.$$

Clearly, $\gcd(9, 17) = 1$. We see that

$$\begin{aligned} 9^{\frac{17-1}{\gcd(48,17-1)}} &= 9^{\frac{16}{\gcd(48,16)}} \\ &= 9^{\frac{16}{16}} \\ &= 9 \\ &\not\equiv 1 \mod 16, \end{aligned}$$

so there are no solutions.

c. We have

$$x^{20} \equiv 13 \mod 17.$$

Clearly, $\gcd(13, 17) = 1$. We see that

$$\begin{aligned} 13^{\frac{17-1}{\gcd(20,17-1)}} &= 13^{\frac{16}{\gcd(20,16)}} \\ &= 13^{\frac{16}{4}} \\ &= 13^4 \\ &\equiv (-4)^4 \\ &= \left((-4)^2\right)^2 \\ &= (16)^2 \\ &\equiv (-1)^2 \\ &= 1 \mod 17, \end{aligned}$$

so there are $\gcd(20, 16) = 4$ solutions.

d. We have

$$x^{11} \equiv 9 \mod 17.$$

Clearly, $\gcd(9, 17) = 1$. We see that

$$\begin{aligned}
9^{\frac{17-1}{\gcd(11,17-1)}} &= 9^{\frac{16}{\gcd(11,16)}} \\
&= 9^{\frac{16}{1}} \\
&= 9^{16} \\
&= \left(9^2\right)^8 \\
&= (81)^8 \\
&\equiv (-4)^8 \\
&= \left((-4)^2\right)^4 \\
&= (16)^4 \\
&\equiv (-1)^4 \\
&= 1 \mod 16
\end{aligned}$$

so there is $\gcd(11, 17) = 1$ solution.

Problem (2.8.10)

Solution.

We see that

$$\begin{aligned}
3^1 &= 3^0 \cdot 3 \equiv 1 \cdot 3 = 3 && \mod 17\\
3^2 &= 3^1 \cdot 3 \equiv 3 \cdot 3 = 9 && \mod 17\\
3^3 &= 3^2 \cdot 3 \equiv 9 \cdot 3 = 27 \equiv 10 && \mod 17\\
3^4 &= 3^3 \cdot 3 \equiv 10 \cdot 3 = 30 \equiv 13 && \mod 17\\
3^5 &= 3^4 \cdot 3 \equiv 13 \cdot 3 = 39 \equiv 5 && \mod 17\\
3^6 &= 3^5 \cdot 3 \equiv 5 \cdot 3 = 15 \equiv 15 && \mod 17\\
3^7 &= 3^6 \cdot 3 \equiv 15 \cdot 3 = 45 \equiv 11 && \mod 17\\
3^8 &= 3^7 \cdot 3 \equiv 11 \cdot 3 = 33 \equiv 16 && \mod 17\\
3^9 &= 3^8 \cdot 3 \equiv 16 \cdot 3 = 48 \equiv 14 && \mod 17\\
3^{10} &= 3^9 \cdot 3 \equiv 14 \cdot 3 = 42 \equiv 8 && \mod 17\\
3^{11} &= 3^{10} \cdot 3 \equiv 8 \cdot 3 = 24 \equiv 7 && \mod 17\\
3^{12} &= 3^{11} \cdot 3 \equiv 7 \cdot 3 = 21 \equiv 4 && \mod 17\\
3^{13} &= 3^{12} \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 12 && \mod 17\\
3^{14} &= 3^{13} \cdot 3 \equiv 12 \cdot 3 = 36 \equiv 2 && \mod 17\\
3^{15} &= 3^{14} \cdot 3 \equiv 2 \cdot 3 = 6 \equiv 6 && \mod 17\\
3^{16} &= 3^{15} \cdot 3 \equiv 6 \cdot 3 = 18 \equiv 1 && \mod 17.
\end{aligned}$$

Consider the congruence $x^n \equiv a \mod p$, for $\gcd(a,p) = 1$ and p is prime, and $n \in \mathbb{Z}^+$. Let g be a primitive root of p. If $g^i \equiv a \mod p$ for $i \in \mathbb{Z}^+$, and $g^u \equiv x \mod p$ for $u \in \mathbb{Z}^+$, then $(g^u)^n = g^{un} = x^n \equiv a \equiv g^i \mod p$, so $un \equiv i \mod (\phi(p) = p-1)$. We can solve for u by application of theorem 2.17.

To find solutions to the congruences in problem 2.8.8, we set $p = 17$, $g = 3$, and see that

a.

$$x^{12} \equiv 16 \mod 17,$$

has solutions $3^u \equiv x \mod (\phi(17) = 16)$ for the congruence $12u \equiv 8 \mod 16$ with $3^8 \equiv 16 \mod 17$. We see that

$$\begin{aligned}
12u &\equiv 8 \mod 16 &&\\
3u &\equiv 2 \mod 4 && \gcd(12,16) = 4, \text{ Theorem 2.3(1)}\\
-u &\equiv 2 \mod 4 &&\\
u &\equiv -2 \mod 4 &&\\
u &\equiv 2 \mod 4, &&
\end{aligned}$$

so the solutions to $u \mod 16$ are $2, 6, 10$, and 14. Thus, the solutions are

$$x \equiv 3^2 \equiv 9 \mod 17$$
$$x \equiv 3^6 \equiv 15 \mod 17$$
$$x \equiv 3^{10} \equiv 8 \mod 17$$
$$x \equiv 3^{14} \equiv 2 \mod 17$$

b.

$$x^{48} \equiv 9 \mod 17,$$

has solutions $3^u \equiv x \mod (\phi(17) = 16)$ for the congruence $48u \equiv 2 \mod 16$ with $3^2 \equiv 9 \mod 17$. We see that

$$48u \equiv 2 \mod 16,$$

has no solutions because $\gcd(48, 16) = 16 \not| 2$, by Theorem 2.17.

c.

$$x^{20} \equiv 13 \mod 17,$$

has solutions $3^u \equiv x \mod (\phi(17) = 16)$ for the congruence $20u \equiv 4 \mod 16$ with $3^4 \equiv 13 \mod 17$. We see that

$$\begin{aligned} 20u &\equiv 4 \mod 16 \\ 5u &\equiv 1 \mod 4 && \gcd(20, 16) = 4, \text{ Theorem 2.3(1)} \\ u &\equiv 1 \mod 4 \end{aligned}$$

so the solutions to $u \mod 16$ are $1, 5, 9$, and 13. Thus, the solutions are

$$x \equiv 3^1 \equiv 3 \mod 17$$
$$x \equiv 3^5 \equiv 5 \mod 17$$
$$x \equiv 3^9 \equiv 14 \mod 17$$
$$x \equiv 3^{13} \equiv 12 \mod 17$$

d.

$$x^{11} \equiv 9 \mod 17,$$

has solutions $3^u \equiv x \mod (\phi(17) = 16)$ for the congruence $11u \equiv 2 \mod 16$ with $3^2 \equiv 9 \mod 17$. We see that

$$11u \equiv 2 \mod 16$$
$$33u \equiv 6 \mod 16$$
$$u \equiv 6 \mod 16$$

so the only solution $u \mod 16$ is 6. Thus, the solution is

$$x \equiv 3^6 \equiv 15 \mod 17$$

Problem (2.8.11)

Solution.

For any number $x \in \mathbb{Z}_{17}$, given that 3 is a primitive root modulo 17, there is some $i \in \mathbb{N}$ such that $x \equiv 3^i \mod 17$. Thus, $x^2 \equiv 3^{2i} \mod 17$. The only numbers for which $x^2 \equiv a$, for $a \in \mathbb{Z}^+$, are those for which the exponent of the primitive root 3 in the congruence $3^k \equiv a \mod 17$ is even. Therefore, the only congruences with solutions are

$$\begin{aligned}
x^2 &\equiv 3^2 \equiv 9 \mod 17 \\
x^2 &\equiv 3^4 \equiv 13 \mod 17 \\
x^2 &\equiv 3^6 \equiv 15 \mod 17 \\
x^2 &\equiv 3^8 \equiv 16 \mod 17 \\
x^2 &\equiv 3^{10} \equiv 8 \mod 17 \\
x^2 &\equiv 3^{12} \equiv 4 \mod 17 \\
x^2 &\equiv 3^{14} \equiv 2 \mod 17 \\
x^2 &\equiv 3^{16} \equiv 1 \mod 17.
\end{aligned}$$

Problem (2.8.13)

Solution.

We aim to show that the numbers $1^k,\ 2^k,\ \ldots,\ (p-1)^k$ form a reduced residue system (mod p) if and only if $\gcd(k, p-1) = 1$.

$\longrightarrow$
Suppose $1^k,\ 2^k,\ \ldots,\ (p-1)^k$ is a reduced residue system. Then for each element a of the set { 1, 2, ..., (p-1) }, the congruence

$$x^k \equiv a \mod p$$

has a solution. By theorem 2.37, solutions for this equation will only exist if

$$a^{\frac{(p-1)}{\gcd(p-1,k)}} \equiv 1 \mod p. \tag{1}$$

By theorem 2.36, and that $\phi(p-1) > 0$ for all primes p, there will always be at least one primitive root whose order is $\phi(p) = p-1$. Let g be a primitive root modulo p. Clearly, $\gcd(g, p) = 1$, because if it were not, $g^k \equiv 0 \mod p$ for all k.

Substituting g for a in equation 1, we see that

$$g^{\frac{(p-1)}{\gcd(p-1,k)}} \equiv 1 \mod p. \tag{2}$$

Clearly, $\frac{(p-1)}{\gcd(p-1,k)} \leq (p-1)$, with equality only when $\gcd(p-1, k) = 1$. Given that the order of g is $p-1$, there will only be a solution to

$$x^k \equiv g \mod p,$$

when $\gcd(k, p-1) = 1$. Since $\gcd(g, p) = 1$, by definition of a reduced residue system, g must be congruent to some member of our assumed reduced residue system. Thus $b^k \equiv g \mod p$ for some $b \in \mathbb{Z}^+$ where $1 \leq b \leq (p-1)$, so equation 2 must be true. Thus, $\gcd(k, p-1) = 1$.

$\longleftarrow$
Suppose $\gcd(k, p-1) = 1$. Let $m, n \in \mathbb{N}$ be such that $m \not\equiv n \mod p$ and $1 \leq m, n \leq (p-1)$ By theorem 2.36, there exists a primitive root modulo p, which we will call g. Because g is a primitive root modulo p, There exist $i, j \in \mathbb{Z}^+$ such that $n \equiv g^i \mod p$ and $m \equiv g^j \mod p$. Using Theorem 2.3(2), we have

$$\begin{aligned}
n &\not\equiv m \mod p \\
g^i &\not\equiv g^j \mod p \\
i &\not\equiv j \mod \phi(p) \\
ik &\not\equiv kj \mod \phi(p) && \text{since } \gcd(k, p-1) = 1 \\
g^{ik} &\not\equiv g^{kj} \mod p \\
\left(g^i\right)^k &\not\equiv \left(g^j\right)^k \mod p \\
n^k &\not\equiv m^k \mod p.
\end{aligned}$$

Furthermore, we note that any positive number less than p is coprime to p. By theorem 1.8, if x is relatively prime to p, then $\gcd(x, p) = \gcd(x^k, p) = 1$.

Since 1, 2, ..., $(p-1)$ are relatively prime to p, so are $1^k, 2^k, \ldots, (p-1)^k$. We already showed that $n^k \not\equiv m^k \mod p$ for $n \not\equiv m \mod p$. Thus, $1^k, 2^k, \ldots, (p-1)^k$ forms a set whose members are distinct, and coprime to p, and of size $\phi(p)$. By definition this is a reduced residue system. $\square$

Problem (2.8.16)

Solution.

We want to show that $\gcd(2^m - 1, 2^n + 1) = 1$ if m is odd.

Call $\gcd(2^m - 1, 2^n + 1) = g$. If $2^m - 1$ and $2^n + 1$ are not coprime, then $g > 1$. By the fundamental theorem of arithmetic, g can be factored into the product of primes and their powers. Let p be one of these prime numbers. Since $p|g$ and $g|(2^m - 1)$ and $g|(2^n + 1)$, $p|(2^m - 1)$ and $p|(2^n + 1)$.

We may write this as

$$2^m - 1 \equiv 0 \mod p \tag{3}$$

$$2^n + 1 \equiv 0 \mod p. \tag{4}$$

We can rewrite the above congruences as

$$2^m \equiv 1 \mod p$$

$$2^{2n} \equiv 1 \mod p.$$

Here, we note that $2^n \equiv -1 \not\equiv 1 \mod p$. Let h denote the order of 2 modulo p. By Lemma 2.31, $h \mid m$ and $h \mid (2n)$. Of course, since $2^n \not\equiv 1 \mod p$, $h \nmid n$. From this we can deduce that h is even because $2n \equiv 0 \mod h$ implies $n \equiv 0 \mod h$ if $\gcd(2, h) = 1$ by Theorem 2.3(2). Since $2n \equiv 0 \mod h$ and $n \not\equiv 0 \mod h$, we see that $\gcd(2, h) \neq 1$. Thus, $\gcd(2, h) = 2$ so $2 \mid h$.

If $h \mid m$, and $2 \mid h$, then $2 \mid m$. But m is odd, so $2 \nmid m$, which implies that $h \nmid m$. Since p was arbitrary and we have shown that equations 3 and 4 cannot simultaneously be true, we see that there is no common divisor of $2^m - 1$ and $2^n + 1$ for odd m, meaning that they are coprime.

Problem (2.8.19)

Solution.

First we aim to show that if $a^h \equiv 1 \mod p$ then $a^{ph} \equiv 1 \mod p^2$.

By definition, $a^h \equiv 1 \mod p$ implies $a^h = np + 1$ for some $n \in \mathbb{Z}$. We see that

$$\begin{aligned}
a^{ph} &= \left(a^h\right)^p \\
&= (np+1)^p \\
&= \sum_{k=0}^{p} \binom{p}{k} (np)^k && \text{Theorem 1.22, the binomial theorem} \\
&\equiv \binom{p}{0} + \binom{p}{1}(np) \mod p^2 && (*) \\
&= 1 + \binom{p}{1}(np) \\
&= 1 + np^2 \\
&\equiv 1 \mod p^2,
\end{aligned}$$

where $(*)$ follows because $\binom{p}{k}(np)^k \equiv 0 \mod p^2$ for $k \geq 2$. □

Second, we aim to prove that if g is a primitive root modulo p^2 then it is also a primitive root moduluo p.

Since g is a primitive root modulo p^2, for every $k \in \mathbb{Z}^+$ and $1 \leq k \leq p-1$, there is some $i \in \mathbb{Z}^+$ such that $g^i \equiv k \mod p^2$. Note that if $g^i \equiv k \mod p^2$, then $g^i \equiv k \mod p$. Suppose the order of g were h modulo p. Then g could only generate h unique values in $\mathbb{Z}_p$. Since g can generate at least $p-1$ values in $\mathbb{Z}_p$, the order of g is at least $p-1$. Furthermore, the order of any element in $\mathbb{Z}_p$ cannot be any larger than $\phi(p) = p-1$, so the order of g must be $p - 1 = \phi(p)$ modulo p. By definition, g is also a primitive root modulo p. □

Problem (2.8.21)

Solution.

Let g be a primitive root of the odd prime p. We aim to show that $-g$ is a primitive root, or not, according as $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$.

Suppose $p \equiv 3 \mod 4$. We see that

$$\begin{aligned}\frac{p-1}{2} &= \frac{p-3+2}{2} \\ &= \frac{p-3}{2} + 1.\end{aligned}$$

Since $p \equiv 3 \mod 4$, by definition $4 \mid p-3$, so $2 \mid \frac{p-3}{2}$ and $\frac{p-1}{2}$ is even. Thus, $\frac{p-1}{2} = \left(\frac{p-3}{2} + 1\right)$ is an odd number. Since g is a primitive root modulo p, the lowest exponent k such that $g^k \equiv 1$ is $k = \phi(p) = p - 1$. From lemma 2.10, we know that the only solutions to the congruence $x^2 \equiv 1 \mod p$ for prime p are $x \equiv \pm 1 \mod p$. Since $\left(g^{\frac{p-1}{2}}\right)^2 \equiv 1 \mod p$, we see that for $g^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Since g is a primitive root, $g^{\frac{p-1}{2}} \equiv -1 \mod p$. However, we see that for $-g$,

$$\begin{aligned}(-g)^{\frac{p-1}{2}} &= (-1)^{\frac{p-1}{2}} g^{\frac{p-1}{2}} \\ &= -1 \cdot -1 \\ &= 1 \mod p,\end{aligned}$$

so the order of $-g$ is less than $p-1 = \phi(p)$ and $-g$ cannot be a primitive root modulo p. $\square$

Suppose that $p \equiv 1 \mod 4$. We will show that $-g$ is a primitive root by showing that any number $a \in \mathbb{Z}_p$ can be represented as $(-g)^k \equiv a \mod p$, for $k \in \mathbb{N}$. This will tell us that the order of $-g$ is at least $p - 1 = \phi(p)$, and combined with Euler's theorem, that the order of $-g$ is $\phi(p)$. We see that sequence generated by $-g$ is

$$-g, g^2, -g^3, g^4, \ldots, g^{2n}, -g^{2n+1} \qquad\qquad n \in \mathbb{Z}^+$$

If $a \in \mathbb{Z}$ can be written as $g^{2k} \equiv a \mod p$ for $k \in \mathbb{N}$, then

$$(-g)^{2k} \equiv (-1)^{2k} g^{2k} \equiv g^{2k} \equiv a \mod p.$$

From theorem 2.12, we know that $x^2 \equiv -1 \mod p$ has a solution for a prime p because $p \equiv 1 \mod 4$. Let $g^k \equiv x \mod p$ be the solution that that congruence for some $k \in \mathbb{N}$. We see that

$$\begin{aligned}x^2 &\equiv -1 \mod p \\ (g^k)^2 &\equiv -1 \mod p \\ g^{2k} &\equiv -1 \mod p \\ g^{2k+1} &\equiv -g \mod p.\end{aligned}$$

From this we can prove any $a \in \mathbb{Z}_p$ which can represented as the primitive root g to an odd power can also be represented as $-g$ to an odd power. To see this, suppose $g^{2l+1} \equiv a \mod p$, for some $l \in \mathbb{N}$. We see that

$$\begin{aligned}
a &\equiv g^{2l+1} \mod p \\
&= g^{2l+1+(2k+1)-(2k+1)} \\
&= g^{2k+1+(2l-2k)} \\
&\equiv g^{2k+1+2(l-k)+n\cdot\phi(p)} \mod p \\
&= g^{2k+1} g^{2(l-k)+n\cdot\phi(p)} && 2(l-k)+n\cdot\phi(p) \geq 0 \\
&\equiv -g \cdot g^{2(l-k)+n\cdot\phi(p)} \mod p \\
&= -g \cdot (-g)^{2(l-k)+n\cdot\phi(p)} && 2(l-k)+n\cdot\phi(p) \equiv 0 \mod 2 \\
&= (-g)^{2(l-k)+n\cdot\phi(p)+1}, && \equiv (-g)^{2q+1} \mod p,
\end{aligned}$$

where $q = (l-k) + n\frac{\phi(p)}{2}$. We note that q is an integer because $\phi(p) = p-1$ must be even considering $p \equiv 1 \mod 4$ so $p \neq 2$. From this we can represent any number a which is an odd power of g as an odd power of $-g$. Since we can generate any non-zero element of $\mathbb{Z}_p$ from $-g$, we conclude $-g$ has an order of at least $p-1$. Since any non-zero element in $\mathbb{Z}_p$ has an order of at most $\phi(p) = p-1$, the order of $-g$ is $p-1 = \phi(p)$. By definition, $-g$ is a primitive root modulo p. $\square$

Problem (2.9.1)

Solution.

a. We want to reduce

$$4x^2 + 2x + 1 \equiv 0 \mod 5$$

into the form $x^2 \equiv a \mod 5$. We have

$$\begin{aligned} 4x^2 + 2x + 1 &\equiv 0 \mod 5 \\ 16(4x^2 + 2x + 1) &\equiv 16 \cdot 0 \mod 5 \\ 64x^2 + 32x + 16 &\equiv 0 \mod 5 \\ (8x + 2)^2 - 4 + 16 &\equiv 0 \mod 5 \\ (8x + 2)^2 + 12 &\equiv 0 \mod 5 \\ (8x + 2)^2 &\equiv -12 \mod 5 \\ (8x + 2)^2 &\equiv 3 \mod 5. \end{aligned}$$

If we substitute $v \equiv 8x + 2 \mod 5$, we can write our congruence as

$$v^2 \equiv 3 \mod 5.$$

Since we can easily solve a linear congruence, we have effectively reduced the problem to solving a congruence of the form $x^2 \equiv a \mod p$

Problem (2.9.7)

Solution.

For $\gcd(a,p)=1$, and $p \equiv 2 \mod 3$ for a prime p, we aim to show the congruence $x^3 \equiv a \mod p$ has the unique solution $x \equiv a^{\frac{2p-1}{3}} \mod p$.

First we show that $\gcd(p-1,3)=1$. Since $p \equiv 2 \mod 3$, we see that $p-1 \equiv 1 \mod 3$ so $3 \nmid (p-1)$. Since 3 is prime, $\gcd(p-1,3)$ is 1 or 3. We have showed that 3 is not a common divisor, so $\gcd(p-1,3)=1$. Theorem 2.37 tells us that there will be a unique solution because $\gcd(p-1,3)=1$ and

$$\begin{aligned} a^{\frac{p-1}{\gcd(p-1,3)}} &= a^{p-1} \\ &\equiv 1 \mod p \qquad \text{(Fermat's little theorem)} \end{aligned}$$

Next we show that $x \equiv a^{\frac{2p-1}{3}} \mod p$ is a solution. We have

$$\begin{aligned} x^3 &\equiv \left(a^{\frac{2p-1}{3}}\right)^3 \mod p \\ &= a^{2p-1} \\ &= a^p \cdot a^{p-1} \\ &\equiv a \cdot 1 \qquad \text{Fermat's little theorem} \\ &\equiv a \mod p. \end{aligned}$$

Therefore, $x \equiv a^{\frac{2p-1}{3}} \mod p$ is the only solution.

Problem (3.1.7)

Solution.

a. We have
$$x^2 \equiv 2 \mod 61.$$
Solutions will exist contingent on the value of $\left(\frac{2}{61}\right)$. We see that the sequence of smallest positive residues of $1 \cdot 2, 2 \cdot 2, \ldots, \frac{61-1}{2} \cdot 2$ is $2, 4, 6, \ldots, 60$. We see that the number of :w elements, n, in the sequence larger than $\frac{61}{2} = 30.5$ is the size of the set $\{32, 34, \ldots, 60\}$. The size of the set is $\frac{60-32}{2} + 1 = 15$. So $n = 15$.

According to theorem 3.2,
$$\begin{aligned}\left(\frac{2}{61}\right) &= (-1)^n \\ &= (-1)^{15} \\ &= -1,\end{aligned}$$
so 2 is a quadratic nonresidue modulo 61 and there are no solutions.

b. We have
$$x^2 \equiv 2 \mod 59.$$
Solutions will exist contingent on the value of $\left(\frac{2}{59}\right)$. We see that the sequence of smallest positive residues of $1 \cdot 2, 2 \cdot 2, \ldots, \frac{59-1}{2} \cdot 2$ is $2, 4, 6, \ldots, 58$. We see that the number of elements, n, in the sequence larger than $\frac{59}{2} = 29.5$ is the size of the set $\{30, 32, 34, \ldots, 58\}$. The size of the set is $\frac{58-30}{2} + 1 = 15$. So $n = 15$.

According to theorem 3.2,
$$\begin{aligned}\left(\frac{2}{59}\right) &= (-1)^n \\ &= (-1)^{15} \\ &= -1,\end{aligned}$$
so 2 is a quadratic nonresidue modulo 59 and there are no solutions.

c. We have

$$x^2 \equiv -2 \mod 61.$$

Solutions will exist contingent on the value of $\left(\frac{-2}{61}\right)$. Using our work in part (a) and theorem 3.1, we see that

$$\begin{aligned}\left(\frac{-2}{61}\right) &= \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right) \\ &= (-1)^{\frac{61-1}{2}}(-1) \\ &= (-1)^{30}(-1) \\ &= 1 \cdot (-1) \\ &= -1,\end{aligned}$$

so -2 is a quadratic nonresidue modulo 61 and there are no solutions.

d. We have

$$x^2 \equiv -2 \mod 59.$$

Solutions will exist contingent on the value of $\left(\frac{-2}{59}\right)$. Using our work in part (b) and theorem 3.1, we see that

$$\begin{aligned}\left(\frac{-2}{59}\right) &= \left(\frac{-1}{59}\right)\left(\frac{2}{59}\right) \\ &= (-1)^{\frac{59-1}{2}}(-1) \\ &= (-1)^{29}(-1) \\ &= (-1) \cdot (-1) \\ &= 1,\end{aligned}$$

so -2 is a quadratic residue modulo 59. If x is a solution modulo 59, $-x$ is also a solution. By theorem 2.26, the number of solutions to the above congruence is bounded by 2. Thus, there are two solutions.

e. We have

$$x^2 \equiv 2 \mod 122.$$

Using theorem 2.3(3) and the factorization $122 = 61 \cdot 2$, we see that this is equivalent to the set of linear congruences

$$\begin{aligned}x^2 &\equiv 2 \mod 61 \\ x^2 &\equiv 2 \mod 2.\end{aligned}$$

The first congruence has no solution so there is no common solution and hence no solution to our original congruence.

f. We have

$$x^2 \equiv 2 \mod 118.$$

Using theorem 2.3(3) and the factorization $118 = 59 \cdot 2$, we see that this is equivalent to the set of linear congruences

$$\begin{aligned}x^2 &\equiv 2 \mod 59 \\ x^2 &\equiv 2 \mod 2.\end{aligned}$$

The first congruence has no solution so there is no common solution and hence no solution to our original congruence.

g. We have

$$x^2 \equiv -2 \mod 122.$$

Using theorem 2.3(3) and the factorization $122 = 61 \cdot 2$, we see that this is equivalent to the set of linear congruences

$$x^2 \equiv -2 \mod 61$$
$$x^2 \equiv -2 \mod 2.$$

The first congruence has no solution so there is no common solution and hence no solution to our original congruence.

h. We have

$$x^2 \equiv -2 \mod 118.$$

Using theorem 2.3(3) and the factorization $122 = 59 \cdot 2$, we see that this is equivalent to the set of linear congruences

$$x^2 \equiv -2 \mod 59$$
$$x^2 \equiv -2 \mod 2.$$

Since we have shown that the first congruence has two solutions, two solutions will exist if they are even or there will be no solutions of they are odd. Suppose that the solutions are even, then

$$\begin{aligned} x^2 &\equiv -2 \mod 59 \\ \frac{1}{2}x^2 &\equiv -1 \mod 59 \\ \frac{1}{2}x^2 &\equiv 58 \mod 59 \\ \frac{1}{4}x^2 &\equiv 29 \mod 59 \\ \left(\frac{x}{2}\right)^2 &\equiv 29 \mod 59. \end{aligned}$$

Thus, if solutions exist to $y^2 \equiv 29 \mod 59$, then the solutions to our original congruence are $\pm 2y$. From theorem 2.37, solutions will exist if

$$\begin{aligned} 29^{\frac{59-1}{\gcd(2,59-1)}} &= 29^{\frac{58}{2}} \\ &= 29^{29} \\ &\equiv 1 \mod 59. \end{aligned}$$

The computation is not the point of the problem so I will state that the above congruence has been verified by computer. Thus, the solution to $x^2 \equiv -2 \mod 59$ is even and also satisfies the congruence $x^2 \equiv -2 \mod 2$, so by theorem 2.3(3), it also is a solution to $x^2 \equiv -2 \mod 122$. There are two solutions.

Problem (3.1.11)

Solution.

Let g be a primitive root of an odd prime p. By definition 3.1, we see that a where $\gcd(a, p) = 1$, will be a quadratic residue or a quadratic nonresidue modulo p accordingly as $\left(\frac{a}{p}\right)$ is 1 or -1, respectively.

Suppose a is a quadratic residue. From theorem 3.1,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}.$$

Let $g^i \equiv a \mod p$ for some $i \in \mathbb{N}$. We see that

$$\begin{aligned} a^{\frac{p-1}{2}} &= \left(g^i\right)^{\frac{p-1}{2}} \\ &= g^{\frac{i(p-1)}{2}}. \end{aligned}$$

Since a is a quadratic residue modulo p,

$$g^{\frac{i(p-1)}{2}} = 1.$$

By definition, the order of g is $\phi(p) = p - 1$. By lemma 2.31, the order of g must divide $\frac{i(p-1)}{2}$. We see that for $(p-1) \mid \frac{i}{2}(p-1)$, $\frac{i}{2}$ must be an integer, which is only true when $2 \mid i$. Thus, $a \equiv g^i \mod p$ for an even i. □

Now suppose a is a quadratic nonresidue. Going by our previous work, if $a \equiv g^i \mod p$ for some $i \in \mathbb{N}$, then

$$g^{\frac{i(p-1)}{2}} = -1.$$

By lemma 2.31, the order of g cannot divide $\frac{i(p-1)}{2}$. We see that $(p-1) \nmid \frac{i}{2}(p-1)$ if $\frac{i}{2}$ is not an integer. This implies $2 \nmid i$. By definition, i is odd. Thus, $a \equiv g^i \mod p$ for an odd i. □

Problem (3.1.12)

Solution.

Let r denote quadratic residues and let n denote quadratic nonresidues modulo p where p is an odd prime.

By theorem 3.1, we see that

$$\begin{aligned}\left(\frac{r_1 r_2}{p}\right) &= \left(\frac{r_1}{p}\right)\left(\frac{r_2}{p}\right)\\ &= 1 \cdot 1\\ &= 1.\end{aligned}$$

By definition, $r_1 r_2$ is a quadratic residue modulo p.

Next, we see that

$$\begin{aligned}\left(\frac{n_1 n_2}{p}\right) &= \left(\frac{n_1}{p}\right)\left(\frac{n_2}{p}\right)\\ &= (-1) \cdot (-1)\\ &= 1.\end{aligned}$$

By definition, $n_1 n_2$ is a quadratic residue modulo p.

Now we see that

$$\begin{aligned}\left(\frac{rn}{p}\right) &= \left(\frac{r}{p}\right)\left(\frac{n}{p}\right)\\ &= 1 \cdot (-1)\\ &= -1.\end{aligned}$$

By definition, rn is a quadratic nonresidue modulo p.

As an example, consider $\mathbb{Z}_{12}$. We see that

$$\begin{aligned}1^2 &\equiv 1 \mod 12\\ 2^2 &\equiv 4 \mod 12\\ 3^2 &\equiv 9 \mod 12\\ 4^2 = 16 &\equiv 4 \mod 12\\ 5^2 = 25 &\equiv 1 \mod 12\\ 6^2 = 36 &\equiv 0 \mod 12\\ 7^2 = 49 &\equiv 1 \mod 12\\ 8^2 = 64 &\equiv 4 \mod 12\\ 9^2 = 81 &\equiv 9 \mod 12\\ 10^2 = 100 &\equiv 4 \mod 12\\ 11^2 = 121 &\equiv 1 \mod 12.\end{aligned}$$

From this, we see that only $0, 1, 4$, and 9 are quadratic residues modulo 12. Clearly, 2 and 3 are quadratic nonresidues modulo 12, and their product, 6, is not a quadratic residue modulo 12.