Throughout, \( \mathbb{N} \) (resp., \( \mathbb{Z} \)) denotes the set of positive integers (resp., all integers). The notation \( a \mid b \) is to be read “\( a \) divides \( b \).” By “prime number,” we always mean “positive prime number.” For all \( m \in \mathbb{Z} \), we write \( U_m \) to denote the group \((\mathbb{Z}/m\mathbb{Z})^\times\) of units modulo \( m \).

**Exercise 1**

Find all \( x \in \mathbb{Z} \) such that \( x \equiv 10 \pmod{24} \) and \( x \equiv 16 \pmod{18} \).

The solutions are precisely those \( x \) that can be written as \( 10 + 24k = 16 + 18\ell \) for some \( k, \ell \). Rearranging gives \( 24k - 18\ell = 6 \), which is equivalent to \( 4k - 3\ell = 1 \). We see \( (k, \ell) = (1,1) \) is a solution, and moreover, any other solution must take the form \( (1 + 3t, 1 - 4t) \) because we require \( 4k \equiv 1 \pmod{3} \) and \( -3\ell \equiv 1 \pmod{4} \). So the general solution to \( x \) takes the form

\[
10 + 24(1 + 3t) = 16 + 18(1 - 4t)
\]

(1)

for some \( t \in \mathbb{Z} \); that is, \( x \equiv 34 \pmod{72} \).

**Exercise 2**

Find all \( x \in \mathbb{Z} \) such that \( x \equiv 8 \pmod{9} \) and \( x \equiv 31 \pmod{33} \).

Observe that \( \gcd(9,33) = 3 \). Observe also that \( 8 \equiv 2 \pmod{3} \) and \( 31 \equiv 1 \pmod{3} \). Therefore, by Exercise 3, there are no solutions to the system.

**Exercise 3**

Prove that there exists \( x \in \mathbb{Z} \) such that \( x \equiv m \pmod{a} \) and \( x \equiv n \pmod{b} \) if and only if \( m \equiv n \pmod{\gcd(a,b)} \). In this case, find the general form of the solution.

In what follows, let \( c = \text{lcm}(a,b) \) and \( d = \gcd(a,b) \).

To show the “only if” direction: \( x \equiv m \pmod{a} \) and \( x \equiv n \pmod{b} \) respectively imply \( x \equiv m \pmod{d} \) and \( x \equiv n \pmod{d} \), giving \( m \equiv n \pmod{d} \).

To show the “if” direction: Suppose \( m, n \) belong to the same residue class modulo \( d \). We will show there is a unique residue class \( x \) modulo \( c \) such that \( x \equiv m \pmod{a} \) and \( x \equiv n \pmod{b} \). Since \( m \equiv n \pmod{d} \), Bézout’s Theorem lets us choose \( k, \ell \in \mathbb{Z} \) such that \( ak - b\ell = n - m \), whence \( m + ak = n + b\ell \). So taking \( x \) to be the residue modulo \( c \) proves existence. If \( x' \) is another value such that \( x' \equiv m \pmod{a} \) and \( x' \equiv n \pmod{b} \), then \( x - x' \) is a multiple of both \( a \) and \( b \), so it is a multiple of \( c \), i.e., \( x' \equiv x \pmod{c} \), which proves uniqueness.

**Remark 1.** In the language of category theory, our solution proves that the commutative diagram

\[
\begin{array}{cc}
\mathbb{Z}/\text{lcm}(a,b)\mathbb{Z} & \rightarrow & \mathbb{Z}/a\mathbb{Z} \\
\downarrow & & \downarrow \\
\mathbb{Z}/b\mathbb{Z} & \rightarrow & \mathbb{Z}/\gcd(a,b)\mathbb{Z}
\end{array}
\]

(2)
of rings is cartesian (alternately, a pullback diagram) for arbitrary integers $a$ and $b$. This result is a generalization of the Chinese Remainder Theorem.

**Exercise 4**

Solve the system of congruences:

\[
\begin{align*}
2x + 3y &\equiv 1 \\ 5x + 10y &\equiv 2
\end{align*} \quad \text{(mod 17)}
\]

Since $2, 5$ are invertible modulo $17$, scaling the first congruence by $5$ and the second by $2$ gives

\[
\begin{align*}
10x + 15y &\equiv 5 \\ 10x + 20y &\equiv 4
\end{align*} \quad \text{(mod 17)}
\]

Subtracting, $-5y \equiv 1 \pmod{17}$, whence $y \equiv 10(-5y) \equiv 10 \pmod{17}$. Therefore, $2x \equiv 1 - 3y \equiv -29 \equiv 5 \pmod{17}$, whence $x \equiv 9(2x) \equiv 9(5) \equiv 45 \equiv 11 \pmod{17}$.

**Exercise 5**

Solve the system of congruences:

\[
\begin{align*}
2x + 3y &\equiv 1 \\ 6x + 10y &\equiv 2
\end{align*} \quad \text{(mod 24)}
\]

Since the coefficients in the second congruence are all even, the given system is equivalent to a system modulo $24/2 = 12$, namely:

\[
\begin{align*}
2x + 3y &\equiv 1 \\ 3x + 5y &\equiv 1
\end{align*} \quad \text{(mod 12)}
\]

But $12 = 2^2 \cdot 3$, so by the Chinese Remainder Theorem, it suffices to solve the system modulo $2^2 = 4$ and $3$ simultaneously:

\[
\begin{align*}
2x + 3y &\equiv 1 \\ 3x + y &\equiv 1
\end{align*} \quad \text{(mod 4)} \quad \begin{align*}
2x &\equiv 1 \\ 2y &\equiv 1
\end{align*} \quad \text{(mod 3)}
\]

The congruences modulo $3$ yield $x, y \equiv 2 \pmod{3}$. Regarding the congruences modulo $4$, we rescale the second by $3$ to get

\[
\begin{align*}
2x + 3y &\equiv 1 \\ x + 3y &\equiv 3
\end{align*} \quad \text{(mod 4)}
\]

Subtracting, $x \equiv 2 \pmod{4}$, whence $3y \equiv 1 - 2x \equiv 1 \pmod{4}$, whence $y \equiv 3 \pmod{4}$. Altogether, we must simultaneously solve

\[
\begin{align*}
x &\equiv 2 \\ y &\equiv 3
\end{align*} \quad \text{(mod 4)} \quad \begin{align*}
x &\equiv 2 \\ y &\equiv 2
\end{align*} \quad \text{(mod 3)}
\]

Whether by brute force, or by the methods developed in the first half of this course, one can verify that the only solution is $(x, y) \equiv (2, 11) \pmod{12}$. 
Exercises 6

Solve \( x^2 \equiv 61 \pmod{100} \).

Since 100 = 4 \cdot 25, it suffices to solve \( x^2 \equiv 61 \pmod{4} \) and \( x^2 \equiv 61 \pmod{25} \) simultaneously. We check that \( x^2 \equiv 61 \equiv 1 \pmod{4} \) if and only if \( x \equiv \pm 1 \pmod{4} \). To solve \( x^2 \equiv 61 \equiv 11 \pmod{25} \), we apply Hensel lifting. Observe that the solutions of \( x^2 \equiv 11 \pmod{5} \) are \( x \equiv \pm 1 \pmod{5} \). Since \( d \frac{d}{dx}(x^2 - 11) = 2x \),

which is nonzero for \( x \equiv \pm 1 \), Hensel’s Theorem says there are unique solutions to \( x^2 - 11 \equiv 0 \pmod{25} \) that respectively lift \( +1 \) and \( -1 \pmod{5} \). Since these lifts take the form \( \pm 1 + 5k \pmod{25} \), we can quickly check that the respective lifts are \( +6 \) and \( -6 \pmod{25} \).

Altogether, it remains to solve the system

\[
\begin{cases}
    x \equiv +1 \text{ or } -1 \pmod{4} \\
    x \equiv +6 \text{ or } -6 \pmod{25}.
\end{cases}
\]

(11)

To reiterate, the integers \( x \) such that \( x^2 \equiv 61 \pmod{100} \) are precisely the integers \( x \) such that \( (x \equiv \pm 1 \pmod{4}) \) and \( (x \equiv \pm 6 \pmod{25}) \). We therefore have to contend with four pairs of linear congruences, corresponding to the possible combinations of signs, which we can solve by the usual methods to get

\[
\begin{align*}
    (\pm 1, \pm 6) & \implies x \equiv \mp 19 \pmod{100}. \\
    (\pm 1, \mp 6) & \implies x \equiv \pm 61 \pmod{100}.
\end{align*}
\]

(12)

(13)

Exercises 7

Solve \( x^2 \equiv 61 \pmod{1000} \).

By Exercise 6, \( x \equiv \pm 19 + 100k \) or \( \pm 69 + 100k \pmod{1000} \) for some \( k \in \mathbb{Z} \), where we can assume \( 0 \leq k < 9 \). In general, we see

\[
(a + 100k)^2 \equiv a^2 + 200ak + 100^2k^2 \equiv a^2 + 200ak \equiv (a + 100(k + 5))^2 \pmod{1000},
\]

so for the purpose of solving for \( x \), we can even assume \( 0 \leq k < 4 \). Testing all possibilities shows there are no solutions, whether \( a \equiv 19 \) or \( a \equiv 69 \).

Exercises 7.20

Fix \( r \in \mathbb{N} \). Show that there are infinitely many primes congruent to 1 modulo \( 2^r \).

Remark 2. The solution on page 271 of [JJ] appears either to have a serious omission or to be in error. Contact me for further details. The following solution is a “fix” to the one there. The key change is Lemma 3, which was suggested in discussion with Karl Schaefer, my officemate.

Suppose there are only finitely many primes congruent to 1 modulo \( 2^r \). Let

\[
a = 2 \prod_{p \equiv 1 \pmod{2^r}} p,
\]

and let \( m = a^{2^r - 1} + 1 \), an odd number. Then the first \( 2^r - 1 \) powers of \( a \) modulo \( m \) have distinct residues and \( a^{2^r - 1} \equiv 1 \pmod{m} \), so the residue of \( a \) modulo \( m \) has order \( 2^r \).

Lemma 3. Let \( G_1, \ldots, G_s \) be groups. If \( G \cong G_1 \times \cdots \times G_s \) and \( a \in G \) has order \( P^r \), where \( P \) is prime, then the projection of \( a \) on \( G_i \) must have order \( P^r \) for some index \( i \).
Proof. Let \( \pi_i : G \to G_i \) be the projection map, a group homomorphism. As the order of \( \pi_i(a) \) in \( G_i \) must divide the order of \( a \) in \( G \), the former must be \( P^r_i \) for some \( r_i \leq r \). It remains to prove that \( r_i = r \) for some \( i \). Indeed, since

\[
\prod_i \pi_i : G \to \prod_i G_i
\]

is an isomorphism, the order of \( a \) in \( G \) is the order of \( \prod_i a_i \) in \( \prod_i G_i \). The latter is \( \max_i P^{r_i} \), so we require

\[
\max_i r_i = r,
\]

whence the result. \( \square \)

Let \( m = q_1^{e_1} \cdots q_k^{e_k} \) be the unique prime factorization of \( m \). Applying Lemma 3 with \( G_i = U_{q_i^{e_i}} \) and \( G = U_m \) and \( P = 2 \), there exists some prime power \( p^r \mid m \) such that the residue of \( a \) modulo \( p^r \) still has order \( 2^r \). Now, \( 2^r \) divides \( \varphi(p^r) = p^r - 1 \). But \( p^r - 1 \) is odd, because it divides \( m \) and \( m \) is odd. Therefore, \( 2^r \) must divide \( p - 1 \). But by construction, \( m \) is not divisible by any prime \( p \) such that \( p \equiv 1 \pmod{2^r} \), so we have a contradiction.

**Exercise 7.21**

For which \( n \) is it true that \(-1\) is a quadratic residue modulo \( n \)?

Suppose \( n = p_1^{e_1} \cdots p_k^{e_k} \) is the unique prime factorization of \( n \). By the Chinese Remainder Theorem, \( x^2 \equiv -1 \pmod{n} \) is solvable if and only if \( x^2 \equiv -1 \pmod{p_i^{e_i}} \) is solvable for each \( i \). So it remains to handle the situation of prime-power modulus, which we summarize in the following lemma:

**Lemma 4.** Let \( p \) be prime, and let \( e \in \mathbb{N} \). Then \( x^2 \equiv -1 \pmod{p^e} \) is solvable for \( x \) if and only if either of the following hold:

\[
\begin{align*}
(1) & \quad p = 2 \text{ and } e = 1. \\
(2) & \quad p \equiv 1 \pmod{4}. 
\end{align*}
\]

**Proof.** For \( p = 2 \). In this case, we must show that \( x^2 \equiv -1 \pmod{2^e} \) is solvable if and only if \( e = 1 \). Indeed, if \( e = 1 \), then we solve it by taking \( x \equiv 1 \). But if \( e = 2 \), then there are no solutions, so there are also no solutions for \( e > 2 \). \( \square \)

**First proof for odd \( p \).** In this case, we must show that \( x^2 \equiv -1 \pmod{p^e} \) is solvable if and only if \( p \equiv 1 \pmod{4} \). For \( e = 1 \), this result is precisely Corollary 7.7 of [J]. For all \( e \geq 2 \), the unsolvability of \( x^2 \equiv -1 \pmod{p} \) implies its unsolvability modulo \( p^e \), so it remains to show that the solvability of \( x^2 \equiv -1 \pmod{p} \) implies its solvability modulo \( p^e \), i.e., that the solvability is independent of the exponent \( e \).

Let \( f(x) = x^2 + 1 \). Suppose there exists \( x_1 \in \mathbb{Z} \) such that \( f(x_1) \equiv 0 \pmod{p} \). We will show by induction on \( e \) that, for all \( e \geq 1 \), there exists \( x_e \in \mathbb{Z} \) such that

\[
\begin{align*}
(1) & \quad f(x_e) \equiv 0 \pmod{p^e}, \\
(2) & \quad x_e \not\equiv 0 \pmod{p}.
\end{align*}
\]

The base case holds because \( x_1 \) already satisfies condition (1), and computing \( f(0) \neq 0 \pmod{p} \) shows \( x_1 \neq 0 \pmod{p} \). Suppose \( x_e \) satisfies conditions (1) and (2). By condition (2) and \( p \) being odd, \( f'(x_e) = 2x_e \not\equiv 0 \pmod{p} \), so by Hensel’s Theorem,\(^3\) there exists \( x_{e+1} \in \mathbb{Z} \) such that \( f(x_{e+1}) \equiv 0 \pmod{p^{e+1}} \) and \( x_{e+1} \equiv x_e \pmod{p^e} \). In particular, \( x_{e+1} \equiv x_e \neq 0 \pmod{p} \), which completes the induction.

\(^3\)Theorem 3.6 of my midterm review.
Second proof for odd \( p \). By the structure theorem for unit groups, \( U_{p^e} \) is cyclic of order \( \varphi(p^e) \) for odd prime \( p \) and arbitrary \( e \). Under the isomorphism \( U_{p^e} \cong \mathbb{Z}/\varphi(p^e)\mathbb{Z} \), the congruence \((-1)^2 \equiv 1 \pmod{p^e}\) corresponds to the congruence
\[
2 \cdot \frac{\varphi(p^e)}{2} \equiv 0 \pmod{\varphi(p^e)},
\]
so the element \(-1 \pmod{p^e}\) corresponds to the element \( \varphi(p^e)/2 \pmod{\varphi(p^e)} \) and the congruence
\[
x^2 \equiv -1 \pmod{p^e}
\]
(18) corresponds to the congruence
\[
2x \equiv \frac{\varphi(p^e)}{2} \pmod{\varphi(p^e)}.
\]
But \( \varphi(p^e) = p^e - (p - 1) \) is even, so (19) is solvable if and only if \( \varphi(p^e)/2 \) is also even. The latter occurs if and only if \( (p - 1)/2 \) is even, i.e., \( p \equiv 1 \pmod{4} \).

Altogether, we have shown that \(-1\) is a quadratic residue modulo \( n \) if and only if, for each prime \( p \) of positive exponent \( e \) in the prime factorization of \( n \), we either have \( p = 2 \) and \( e = 1 \), or else, \( p \equiv 1 \pmod{4} \).

Exercise 7.23

Show that if \( n > 2 \), then a quadratic residue modulo \( n \) cannot be a primitive root modulo \( n \).

We prove the contrapositive. Suppose \( x \) is a primitive root of \( U_n \), where \( n > 2 \). Then \( U_n \) is cyclic of order \( \varphi(n) \), i.e., every element is expressible as a power of \( x \). In particular, the quadratic residues modulo \( n \), being the elements of the form \( s^2 \) for some \( s \in U_n \), are precisely the elements expressible as even powers of \( x \).

But \( n > 2 \), so \( \varphi(n) \) is even by Exercise 5.7 of [JJ]. So \( x \) is not expressible as an even power of itself: Indeed, if \( x^1 = x^{2k} \), then \( \varphi(n) \mid (2k - 1) \) because \( \varphi(n) \) is the order of \( n \), but this is impossible because \( 2k - 1 \) is odd. Therefore, \( x \) is not a quadratic residue.

Reference