Please read: I will try to post here a few solutions. The new solutions will be added to this same file. They might come with no explanation, just the “answer”. If yours do not match mine, you can try to figure out again. (Also, read the disclaimer below!) You can come to office hours if you want explanations for the unexplained answers. Be careful that just because our “answers” were the same, it doesn’t mean that you solved the problem correctly (it might have been a “fortunate” coincidence), and in the exams what matters is the solution itself. I will do my best to post somewhat detailed solutions, though.

Disclaimer: I will have to put these solutions together rather quickly, so they are subject to typos and conceptual mistakes. (I expect you to be a lot more careful when doing your HW than I when preparing these.) You can contact me if you think that there is something wrong and I will fix the file if you are correct.

Note: I will use the square brackets “[ ... ]” to include extra explanations and comments which are not quite necessary for the solution, but that should make things a bit more clear.

Section 1.3

1.46 F, T, T, F, T [if \( d \mid n \) and \( d \nmid (n + 1) \), then \( d \mid 1 \), and hence \( d = \pm 1 \)], F [(1, 3) = 1], T, T [the 2-adic digits are 0 and 1 only], F [you need to allow negatives].

1.50 If \( d \mid d' \), then clearly \( |d| \leq |d'| \). Thus, \( |d| \leq |d'| \). Now, in the same way, since \( d' \mid d \), we get that \( |d'| \leq |d| \). Thus \( |d| = |d'| \), which implies that \( d = \pm d' \).
1.53

\[
1000 = 0 + 0 \cdot 2 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5 + 1 \cdot 2^6 + 1 \cdot 2^7 + 1 \cdot 2^8 + 1 \cdot 2^9 \\
= 1 + 0 \cdot 3 + 0 \cdot 3^2 + 1 \cdot 3^3 + 0 \cdot 3^4 + 1 \cdot 3^5 + 1 \cdot 3^6 \\
= 0 + 2 \cdot 4 + 2 \cdot 4^2 + 3 \cdot 4^3 + 3 \cdot 4^4 \\
= 0 + 0 \cdot 5 + 0 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 \\
= 0 + 10 \cdot 20 + 2 \cdot 20^2.
\]

1.55 (i) We have \( d = 3, \ s = 299, \ t = -1530, \) and \( 12327/2409 = 4109/803. \)

1.57 By Theorem 1.35 [which I called Bezout’s Theorem], we have that there are \( r, s \in \mathbb{Z} \) such that
\[
ra + bs = d.
\]
Dividing this equation by \( d, \) we have:
\[
r \left( \frac{a}{d} \right) + s \left( \frac{b}{d} \right) = 1.
\]
Problem 1.56 [done in class], this implies that \( (a/d, b/d) = 1. \)

1.58 Suppose that \( p \) is a prime such that \( p \) divides both \( rr’ \) and \( m. \) [This would mean that \( p \mid (rr’, m), \) and hence we need to get a contradiction.] Since \( p \) is prime, Euclid’s Lemma tells us that either \( p \mid r \) or \( p \mid r’. \) But that means that \( p \) is a common divisor of either \( r \) and \( m \) [as \( p \mid m \) by assumption] or \( r’ \) and \( m. \) But both are impossible as the respective GCDs are 1. Therefore, there is no prime common divisor of \( rr’ \) and \( m. \) Thus \( (rr’, m) = 1 \) [as if it was not one, this GCD would have a prime factor which would also be a common divisor.]

1.60 We have that \( n = aa_1 \) [as \( a \mid n]. \) Since \( b \mid n, \) we have that \( b \mid aa_1, \) and by Corollary 1.40, we have that \( b \mid a_1, \) i.e., \( a_1 = a_2b. \) Thus, \( n = aba_2, \) and therefore \( ab \mid n. \)

1.62 Let \( d = (b, c). \) Now, clearly \( ad \) is a common divisor of \( ab \) and \( ac \) [as \( ab/ad = b/d \) and \( ac/ad = c/d \) are integers]. So, if \( e = (ab, ac), \) then by Corollary 1.36 we have that \( ad \mid e, \) say \( e = adq, \) for some \( q \in \mathbb{Z}. \)

Now, since \( e \) is a common divisor of \( ab \) and \( ac \) we have that \( ab = adqk_1 \) and \( ac = adqk_2, \) which imply that \( b/d = qk_1 \) and \( c/d = qk_2. \) [Note that we know that \( b/d, c/d \in \mathbb{Z}. \)] Hence, \( q \) is a common divisor of \( b/d \) and \( c/d. \) But, by Problem 1.57, we have that
\((b/d, c/d) = 1\), and hence we must have that \(q = \pm 1\). Therefore, \(e = \pm ad\), and since \(e\), \(a\), and \(d\) are positive, we must have \(e = ad\).

### Section 1.4

1.68 F [as two integers differ by less than 1/2 if and only if they are equal, and the two numbers are not equal due to the uniqueness of factorization in the *Fundamental Theorem of Arithmetic*, T, T, T [just that any prime divisor of the GCD], T [look at the factorizations].

1.69(i) \(\gcd(210, 48) = \gcd(2 \cdot 3 \cdot 5 \cdot 7, 2^4 \cdot 3) = 2 \cdot 3 = 6\).

1.70(i) If \(m\) is a perfect square iff \(m = n^2\), where \(n \in \mathbb{Z}\). Since \(m \geq 2\), we can assume that \(n \geq 2\) [as if \(n\) is negative, we can replace it by \(-n\)].

By the *Fundamental Theorem of Arithmetic*, \(n = p_1^{e_1} \cdots p_k^{e_k}\), with \(p_i\) distinct primes and \(e_i > 0\). So, \(m\) is a perfect square iff

\[ m = n^2 = p_1^{2e_1} \cdots p_k^{2e_k}, \quad e_i \in \{1, 2, \ldots\}, \]

i.e., iff the each prime factor \(p_i\) occurs an even number of times [namely, \(2e_i\)].

1.71 We just used the previous one. Since \((a, b) = 1\), the don’t have any common prime divisor [or such prime divisor would be a common divisor greater than 1], and hence we can write:

\[ a = p_1^{e_1} \cdots p_k^{e_k}, \quad b = q_1^{f_1} \cdots q_l^{f_l}, \]

with the \(p_i\)’s and \(q_i\)’s all distinct primes and \(e_i, f_i > 0\). [I.e., the prime decompositions have no common prime.]

Thus,

\[ ab = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_l^{f_l}, \]

and, since \(ab\) is a perfect square, by Problem 1.70(i) we have that each \(e_i\) and \(f_i\) is even. By the same problem, \(a\) and \(b\) are perfect squares.

1.75 We may assume \(a_i \neq 0\) for all \(i\), for if not every common multiple is 0, and the statement is trivial.
[⇒] Suppose that $M = \text{lcm}(a_1, \ldots, a_n)$. Then, if we write:

$$a_1 = p_1^{e_{1,1}} \cdot p_2^{e_{2,1}} \cdots p_k^{e_{k,1}},$$

$$a_2 = p_1^{e_{1,2}} \cdot p_2^{e_{2,2}} \cdots p_k^{e_{k,2}},$$

$$\vdots$$

$$a_n = p_1^{e_{1,n}} \cdot p_2^{e_{2,n}} \cdots p_k^{e_{k,n}},$$

where the $p_i$'s are distinct primes and $e_{i,j}$ are non-negative integers, we have that

$$M = p_1^{M_1} \cdot p_2^{M_2} \cdots p_k^{M_k},$$

where $M_i = \max\{e_{i,1}, e_{i,2}, \ldots, e_{i,n}\}$. Now, let $b$ be a common multiple. [We need to show that $M \mid b$.] Let $i \in \{1, \ldots, n\}$ and suppose that $e_{i,j} = \max\{e_{i,1}, \ldots, e_{i,n}\}$. Then, since $a_j \mid b$, we have that $p_i^{e_{i,j}} = p_i^{M_i} \mid b$. Since this is works for all $i$, and since $(p_i^{M_i}, p_j^{M_j}) = 1$ [as the primes are distinct], by Problem 1.60 above, we have that $M = p_1^{M_1} \cdots p_n^{M_n} \mid b$.

[⇐] Assume now that $m$ is a positive common multiple such that every other common multiple $b$ is such that $m \mid b$, and let $M$ be the LCM, described above. [We must show that $m = M$.] Since we have already proved that for all common multiple $b$ we have $M \mid b$, and $m$ is a common multiple, then $M \mid m$. Also, since $M$ is a common multiple, our assumption tells us that $m \mid M$. Since $m, M > 0$, the two divisibility statements gives us that $m = M$ [by Problem 1.50].

### Section 1.5

**1.77** T, F, F, F, F, T, F, T, F.

**1.78** (ii) We have that $\gcd(7, 10) = 1$ and the extended Euclidean algorithm gives us $3 \cdot 7 + 2 \cdot 10 = 1$. Then, $7x \equiv 4 \pmod{10}$ is equivalent to $x \equiv 2 \pmod{10}$ [by multiplying the former equation by 3]. Thus, the set of solutions is $\{2 + 10k : k \in \mathbb{Z}\}$.

(iii) The extended Euclidean algorithm gives us $182 \cdot 243 + (-61) \cdot 725 = 1$. By multiplying the original equation by 182 [after subtracting $17$ from both sides] and reducing modulo $725$, we obtain $x \equiv 63 \pmod{725}$. So, the solution set is $\{63 + 725k : k \in \mathbb{Z}\}$.
1.79 Let 
\[ m = d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k, \quad m' = e_0 + e_1 \cdot 10 + \cdots + e_k \cdot 10^k, \]
where the \( e_i \)'s are just a rearrangement of the \( d_i \)'s. Then, we must have:
\[ d_0 + d_1 + \cdots + d_k = e_0 + e_1 + \cdots + e_k. \]

Then, since \( 10 \equiv 1 \pmod{9} \),
\[ m \equiv d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k \pmod{9} \]
\[ \equiv d_0 + d_1 + \cdots + d_k \pmod{9} \]
\[ = e_0 + e_1 + \cdots + e_k \]
\[ \equiv e_0 + e_1 \cdot 10 + \cdots + e_k \cdot 10^k \pmod{9} \]
\[ = m'. \]

1.81 We have just reduce modulo 7 in steps:
\[ 10^{100} \equiv 3^{100} \equiv (3^2)^{50} \equiv 4^{25} = (4^5)^5 = (4^2 \cdot 4^3)^5 \equiv (2 \cdot 1)^5 \equiv 4 \pmod{7}. \]

Here is another way of doing it using Theorem 1.65: since 7 is prime, \( a^{7k} \equiv a \pmod{7} \) for all integers \( a \) and \( k \). Then, since \( 100 = 14 \cdot 7 + 2 = 2 \cdot 7^2 + 2 \), we have:
\[ 10^{100} \equiv 3^{7^2 \cdot 2+2} = (3^{7^2})^2 \cdot 2^2 \equiv 3^2 \cdot 3^2 \equiv 2 \cdot 2 = 4 \pmod{7}. \]

There is an even better way using a result I will prove in class: if \( p \) is prime and \( p \nmid a \), then \( a^{p-1} \equiv 1 \pmod{p} \). Then, since \( 100 = 6 \cdot 16 + 4 \), we would have
\[ 10^{100} \equiv 3^{6\cdot16+4} = (3^6)^{16} \cdot 3^4 \equiv 1 \cdot 4 \pmod{7}. \]

1.82(i) We have \( \gcd(10, 7) = 1 \) and \(-2 \cdot 10 + 3 \cdot 7 = 1\). Also, since \( \gcd(2, 7) = 1 \), we have
that \( 7 \mid 10q + r \) iff \( 7 \mid -20q - 2r \). Translating the latter terms of congruences we have \(-20q - 2r \equiv 0 \pmod{7} \) and since \(-20 \equiv 1 \pmod{7} \), that is equivalent to \( q - 2r \equiv 0 \pmod{7} \), i.e., \( 7 \mid q - 2r \).

1.85 As seen in Example 1.61, square modulo 8 are congruent to either 0, 1, or 4. Since \( 999 \equiv 7 \pmod{8} \), and no sum of three among 0, 1, and 4 is congruent to 7 modulo 8, there can be no such \((x, y, z) \in \mathbb{Z}^3\). [Note that there are smarter ways to check that than sheer brute force!]

5
1.86 We just need to check $a^2$ modulo 100. Hence, if $a = a_0 + a_1 \cdot 10 + \cdots$, we have:
\[
a^2 \equiv (a_0 + a_1 \cdot 10)^2 \equiv a_0^2 + 20a_1 \pmod{100}
\]
Since, the only digit whose square ends in 5 is $a_0 = 5$, we must have $25 + 20 \cdot a_1 \equiv 35 \pmod{100}$, which implies $2a_1 \equiv 1 \pmod{10}$ [by subtracting 25 and dividing by 10]. But this congruence has no solution, as $2a_1$ is even and every number congruent to 1 modulo 10 is odd.

1.87 We just need to look at $x$ modulo 12, as $(x+12k)^2 \equiv x^2 + 24kx + 144x^2 \equiv x^2 \pmod{12}$. The numbers described then have to be congruent to 1, 5, 7, 11, and all of those have squares congruent to 1 modulo 24. [Note $7 \equiv -5, 11 \equiv -1 \pmod{12}$]

1.88 $a^2 \equiv 1 \pmod{p}$ iff $p \mid (a^2 - 1) = (a - 1)(a + 1)$. By Euclid’s Lemma, $p \mid (a - 1)$ or $p \mid (a + 1)$. Hence, $a \equiv \pm 1 \pmod{p}$.

1.91 (i) [Here we solve by substitution.] Since $x \equiv 2 \pmod{5}$, we have that $x = 2 + 5k$ for $k \in \mathbb{Z}$. Substituting in the other equation, we obtain $6 + 15k \equiv 1 \pmod{8}$, i.e., $7k \equiv -5 \pmod{8}$. [Now, we could use the extended Euclidean algorithm again, and find that $7 \cdot 7 + 6 \cdot 8 = 1$ and multiply the equation by 7, as done before. But here is another idea that applies in this case only.] That is the same as $-k \equiv -5 \pmod{8}$, which implies that $k \equiv 5 \pmod{8}$. Hence, $k = 5 + 8l$ for $l \in \mathbb{Z}$, which gives us that $x = 27 + 40l$, for $l \in \mathbb{Z}$.

(ii) [Here we will use the other method of solutions.] Remember: If gcd($m_1, m_2$) = 1 and $rm_1 + sm_2 = 1$, then all solutions of
\[
x \equiv b_1 \pmod{m_1}
\]
\[
x \equiv b_2 \pmod{m_2}
\]
are \{b_2rm_1 + b_1sm_2 + km_1m_2 : k \in \mathbb{Z}\}.

So, in this case, we first need to get rid of the coefficients of $x$. Since, $2 \cdot 3 + (-1) \cdot 5 = 1$ and $2 \cdot 2 + (-1) \cdot 3 = 1$, we multiply both equations by 2, obtaining:
\[
x \equiv 4 \pmod{5},
\]
\[
x \equiv 2 \pmod{3}.
\]
Using the extended Euclidean algorithm we obtain \((-1) \cdot 5 + 2 \cdot 3 = 1\), and hence a solution is \(x = 2 \cdot (-1) \cdot 5 + 4 \cdot 2 \cdot 3 = 14\). So, all solutions make the set 
\(\{14 + 15k : k \in \mathbb{Z}\}\).

[Again, we could have solved a bit quicker observing that the equations are]

\[
\begin{align*}
x &\equiv -1 \pmod{5}, \\
x &\equiv -1 \pmod{3}.
\end{align*}
\]

Hence, we could get the solutions set as \(\{-1 + 15k : k \in \mathbb{Z}\}\).]