Solutions to HW #1

1.1: #1 GUVFVFGURZRFFNTR

1.2: #1 1000 = 10 * 99 + 10, so r = 10.

1.2: #15 Let

\[ N = a_k a_{k-1} \cdots a_0, 0 \leq a_j \leq 9, \]

in base 10 so

\[ N = \sum_{j=0}^{k} a_j 10^j. \]

Since 10^j \equiv 0 \mod 100 for j \geq 2,

\[ N \equiv a_0 + 10 * a_1 \mod 100, \]

which has the decimal form of a_1a_0.

#17: If \( N = q * m + r, \) where 1 \( \leq r \leq m - 1, \) then \( -N = -q * m - r = (-1 - q) * m + (m - r), \) where 1 \( \leq m - r \leq m - 1. \)

#18: The multiples of 13 are

13, 26, 39, 52, 65, 78, 91, 104, 117, 130, 143, 156, 169, 182, 195, 208, 221, 234, 247, 260, 273, 286, 299,

so 13 * 23 \equiv -1 \mod 100 and an inverse to 13 is -23 = 77.

1.5: #6: \( 2 * n \equiv 1 \mod 2n - 1 \) so an inverse is 2.

#9: \( n * n \equiv -1 \mod n^2 + 1 \) so an inverse is \(-n \equiv n^2 - n + 1 \mod n^2 + 1. \)

1.6: #4: \( \phi(30) = 30 * (1 - 1/2) * (1 - 1/3) * (1 - 1/5) = 30 * 1/2 * 2/3 * 4/5 = 8. \)

They are \( \{1, 7, 11, 13, 17, 19, 23, 29\} \).

#8: The ones digit is 2, 4, 8, 6 repeating and 99 \equiv 3 \mod 4 so the answer is 8.

#17: Reduce the equation \mod 7: can

\[ x^3 + y^3 \equiv 3 \mod 7? \]

The cubes mod 7 are 0, 1, 6, 1, 6, 6 so only 0, 1, 6. The sum of two of these is never 3 \mod 7.

1.7: #2: "meet me at midnight" is

\[ \{12, 4, 4, 19, 12, 4, 0, 19, 12, 8, 3, 13, 8, 6, 7, 19\} \]

applying 11 * x + 1 gives

\[ \{3, 19, 19, 2, 3, 19, 1, 2, 3, 11, 8, 14, 11, 15, 0, 2\} \]
so the GCD is 347.

#8: Let $A = n^3 + n^2 + n + 1$ and $B = n^2 + n + 1$. Then $A - n \cdot B = 1$, so an integer linear combination of $A$ and $B$ is 1. Thus $\text{GCD}(A, B) = 1$.

E1: Let’s show $2m + n^2 = x^2$ has no integer solution if $m$ is odd by reducing modulo 4. The squares mod 4 are 0 and 1, while $2m \equiv 2 \mod 4$ since $m$ is odd. Is $2 + (0$ or 1) $\equiv (0$ or 1) mod 4 possible? No.

E2: Since $\text{GCD}(a, b) = 1$, let $\alpha a + \beta b = 1$, for integers $\alpha$ and $\beta$. Multiply by $c$:

$$\alpha ac + \beta bc = c.$$ 

$a$ divides the first term, and $a$ divides $bc$, so $a$ must divide $c$.

E3: $m$ is a perfect square if, and only if, the number of divisors of $m$ is odd.

Proof: Let $m = p_1^{e_1} \cdots p_k^{e_k}$ be the prime factorization of $m$. The number of divisors of $m$ is $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$, which is odd exactly when each $e_i$ is even. This occurs exactly when $m$ is a perfect square.

E4: TRUE. We’ll show that $\text{GCD}(\alpha, \beta) = E > 1$ is impossible. Divide both sides by $E$:

$$\frac{\alpha}{E}a + \frac{\beta}{E}b = \frac{d}{E}.$$ 

The left side is an integer linear combination of $a$ and $b$, which is a positive integer $\frac{d}{E} < D$, if $E > 1$. This is impossible.

E5: (a) $\phi(24) = 24 * (1-1/2)* (1-1/3) = 8$, the 8 elements are $\{1, 5, 7, 11, 13, 17, 19, 23\}$.

(b) Since 5 has an inverse mod 24, namely 5 itself, the solution is $x \equiv 5^{-1} \cdot 3 \equiv 15 \mod 24$.

(c) We need to choose an appropriate $\alpha$ which does not have an inverse mod 24, so not relatively prime to 24. For example $\alpha = 3$, let’s just try $3x \equiv 0 \mod 24$, which has solutions $x = 0, 8, 16 \mod 24$.

E6: Let’s try to find $k$ consecutive integers which are divisible by 2, 3, , $k+1$, and greater than $k + 1$. For the first proof we just write down the required
consecutive integers. Well $(k + 1)!$ is much greater than $k + 1$, and it is divisible by any of 2, 3, $\cdots$ $k + 1$. So just take for the $k$ consecutive integers

$$(k + 1)! + 2, (k + 1)! + 3, \ldots, (k + 1)! + (k + 1).$$

For example if $k = 4$ these are 122, 123, 124, 125. This problem says that the gaps between primes can be arbitrarily large.

One may also prove this using the CRT. Let the $k$ consecutive integers be $x, x + 1, \cdots, x + k - 1$. Let the first $k$ primes be $p_1 = 2, p_2 = 3, \cdots, p_k$. Consider the equations

$$x \equiv 0 \mod 2, \quad x + 1 \equiv 0 \mod p_2, \cdots x + k - 1 \equiv 0 \mod p_k$$

Since $x + j - 1$ is divisible by the prime $p_j$, it is not prime as long as it is greater than $p_j$. The CRT solution is a congruence class $x \equiv A \mod p_1 p_2 \cdots p_k$. So large values of $x$ are greater than any prime $p_j$. 