

CSE 311 - HW 5

Eric Boris,

Ardi Madadi, Estevan Seyfried, Sam Vanderlinda, Wendy Jiang

October 2019

1 A Modding Acquaintance

1(a)

Equations with recursive calls:

$$\begin{aligned}\gcd(44, 180) &= \gcd(180, 44 \bmod 180) = \gcd(180, 44) \\ &= \gcd(44, 180 \bmod 44) = \gcd(44, 4) \\ &= \gcd(4, 44 \bmod 4) = \gcd(4, 0) \\ &= 4\end{aligned}$$

Tableau form:

$$\begin{aligned}44 &= 0 * 180 + 44 \\ 180 &= 4 * 44 + 4 \\ 44 &= 11 * 4 + 0\end{aligned}$$

1(b)

Equations with recursive calls:

$$\begin{aligned}\gcd(340, 178) &= \gcd(178, 340 \bmod 178) = \gcd(178, 162) \\ &= \gcd(162, 178 \bmod 162) = \gcd(162, 16) \\ &= \gcd(16, 162 \bmod 16) = \gcd(16, 2) \\ &= \gcd(2, 16 \bmod 2) = \gcd(2, 0) \\ &= 2\end{aligned}$$

Tableau form:

$$\begin{aligned}340 &= 1 * 178 + 162 \\ 178 &= 1 * 162 + 16 \\ 162 &= 10 * 16 + 2 \\ 16 &= 8 * 2 + 0\end{aligned}$$

1(c)

Equations with recursive calls:

(If a is a positive integer, $\gcd(a, 0) = a$.)

$$\gcd(2^{32} - 1, 2^0 - 1) = 2^{32} - 1$$

Tableau form:

$$2^{32} - 1 = NA * 0 + 2^{32} - 1$$

2 Mod Squad

2(a)

Find the gcd(15, 103) in tableau form and solve each equation for r such that $r = a - q * b$

$$\begin{aligned} 15 &= 0 * 103 + 15 \\ 103 &= 6 * 15 + 13 \quad == 103 - 6 * 15 = 13 \\ 15 &= 1 * 13 + 2 \quad == 15 - 1 * 13 = 2 \\ 13 &= 6 * 2 + 1 \quad == 13 - 6 * 2 = 1 \end{aligned}$$

Use backward substitution to solve for $\text{gcd}(a, b) = sa + tb$

$$\begin{aligned} 13 - 6 * 2 &= 1 \\ 13 - 6 * (15 - 1 * 13) &= 1 \\ 13 - 6(15) + 6(13) &= 1 \\ 7(13) - 6(15) &= 1 \\ 7(103 - 6 * 15) - 6(15) &= 1 \\ 7(103) - 42(15) - 6(15) &= 1 \\ 7(103) - 48(15) &= 1 \\ 103(7) + 15(-48) &= 1 \end{aligned}$$

Let $0 \leq a, b < m$. Then b is multiplicative inverse of $a(\text{mod } m)$ iff $ab \equiv 1(\text{mod } m)$.

$$\begin{aligned} 1 &= sa + tm \quad \equiv sa(\text{mod } m) \\ &= 15(-48) + 103(7) \equiv 15(-48)(\text{mod } 103) \end{aligned}$$

Now $(-48) \text{ mod } 103 = 55$. So, 55 is the multiplicative inverse of 15 mod 103.

2(b)

We want to find every integer solution $\{x | x \in \mathbb{Z}\}$ to $15x \equiv 11(\text{mod } 103)$. From above, we already know that the multiplicative inverse of 15 mod 103 is 55. That is $15 \cdot 55 \equiv 1(\text{mod } 103)$. Therefore if x is a solution, multiplying by 55 we have $55 \cdot 15 \cdot x \equiv 55 \cdot 11(\text{mod } 103)$. Multiplying the second congruence by x gives $x \equiv 55 \cdot 15 \cdot x(\text{mod } 103)$. Taking these together we have $x \equiv 55 \cdot 11 \equiv 90(\text{mod } 103)$. This shows that every solution is congruent to 90. Thus, the set of numbers of the form $x = 90 + 103k$ for any k , are exactly solutions of this form.

2(c)

We want to show that there are no integer solutions to the equation $10x \equiv 3 \pmod{15}$. Applying De Morgan's informs us that there are no integer solutions if and only if every $x \in \mathbb{Z}$ is not a solution. To proceed we will show that this is the case with an argument from contradiction. Assume that x is an integer solution to the equation.

2(d)

3 Two Peas In a Mod

3(a)

Compute $3^{338} \bmod 100$ using the efficient modular exponentiation algorithm. The algorithm gives us a solution of the form, $a^{2^i} \bmod m = (a^{2^{i-1}})^{2^i} \bmod m$. However, this is only valid for powers of 2. We can rewrite in that form by converting to binary $338_{10} = 101010010_2$. Then, find the powers of 2 sum expansion for the binary value $338_{10} = (2^1 + 2^4 + 2^6 + 2^8)$. Now we substitute that into the original equation and expand the bases.

$$\begin{aligned} 3^{338} \bmod 100 &= 3^{(2^1+2^4+2^6+2^8)} \bmod 100 \\ &= 3^{(2+16+64+256)} \bmod 100 \\ &= (3^2 * 3^{16} * 3^{64} * 3^{256}) \bmod 100 \end{aligned}$$

Next, calculate mod 100 of the powers of $2 \leq 338$.

$$\begin{aligned} 3^2 \bmod 100 &= 9 \\ \\ 3^{16} \bmod 100 &= (3^8)^2 \bmod 100 &= (3^8 \bmod 100)^2 \bmod 100 \\ &= (61)^2 \bmod 100 &= 3721 \bmod 100 \\ &= 21 \\ 3^{64} \bmod 100 &= (3^{32})^2 \bmod 100 &= (3^{32} \bmod 100)^2 \bmod 100 \\ &= (41)^2 \bmod 100 &= 1681 \bmod 100 \\ &= 81 \\ \\ 3^{256} \bmod 100 &= (3^{128})^2 \bmod 100 &= (3^{128} \bmod 100)^2 \bmod 100 \\ &= (61)^2 \bmod 100 &= 3721 \bmod 100 \\ &= 21 \end{aligned}$$

Wrapping up, we now simply substitute these intermediate values back into the above formula and solve.

$$\begin{aligned}
 3^{338} \bmod 100 &= (3^2 * 3^{16} * 3^{64} * 3^{256}) \bmod 100 \\
 &= (9 * 21 * 81 * 21) \bmod 100 \\
 &= (31752) \bmod 100 \\
 &= 89
 \end{aligned}$$

4 Weekend At Cape Mod

4(a)

Prove that, if $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{d}$, where $d \equiv \gcd(m, n)$. Let a , b , c , d , m , and n be arbitrary integers. Assume $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$. Then, by the definition of modulo we can write $m|a - b$ and $n|a - c$ and by the definition of GCD we know that if d is the GCD of m and n that we can say $d|m$ and $d|n$. If d is a factor of m and n then d also evenly divides anything that m and n evenly divides, or $d|a - b$ and $d|a - c$. From the definition of Modulo we can say that $a \equiv b \pmod{d}$ and $a \equiv c \pmod{d}$. Because Modulo is transitive we can conclude that $a \equiv b \equiv c \pmod{d}$ and by direct proof say that because a , b , c , d , m , and n were arbitrary that $a \equiv b \pmod{d}$ and $a \equiv c \pmod{d}$ imply $b \equiv c \pmod{d}$. \square

5 Master of Induction

Prove by induction that $n^3 + 2n$ is divisible by 3 for any $n > 0$ and $n \in \mathbb{Z}$. The base case, $n = 1$ holds, $3|(1)^3 + 2(1) = 3|3 = 1$. Inductive hypothesis, assume $3|k^3 + 2k$ for an arbitrary integer k . Inductive step, prove $3|(k + 1)^3 + 2(k + 1)$.

$$\begin{aligned}
 3|(k + 1)^3 + 2(k + 1) &= \\
 &= 3|k^3 + 3k^2 + 3k + 2k + 3 \\
 &= 3|(k^3 + 2k) + (3k^2 + 3k + 3) && \text{Inductive Hypothesis} \\
 &= 3|(k^3 + 2k) + 3(k^2 + k + 1)
 \end{aligned}$$

Thus, because the base case was divisible by 3, the second term in the rearranged equation is always divisible by 3, and k was arbitrary, we've shown by induction that $n^3 + 2n$ is always divisible by 3. \square

6 Super Colliding Super Inductor

Prove by induction that for all $n \in \mathbb{R}$ and $x \in \mathbb{Z}$ with $x > -2$, the inequality $(2+x)^n \geq 2^n + n2^{n-1}x$ holds. The base case when $n = 0$ holds, $(2+x)^{(0)} = 1 \geq 1 = 2^{(0)} + (0)2^{(0)-1}x$. Inductive hypothesis, assume $(2+x)^k \geq 2^k + k2^{k-1}x$ for an arbitrary real number k . Inductive step, prove $(2+x)^{(k+1)} \geq 2^{(k+1)} + (k+1)2^kx$.

$$(2+x)^{(k+1)} = \tag{1}$$

$$(2+x)^k(2+x) \geq (2^k + k2^{k-1}x)(2+x) \tag{2}$$

$$(2+x)^{k+1} \geq 2^{k+1} + k2^kx + 2^kx + k2^{k-1}x^2 \tag{3}$$

$$(2+x)^{k+1} \geq 2^{k+1} + (k+1)2^kx + (k2^{k-1}x^2) \tag{4}$$

$$(2+x)^{k+1} \geq 2^{k+1} + (k+1)2^kx + (k2^{k-1}x^2) \geq 2^{(k+1)} + (k+1)2^kx \tag{5}$$

We begin with the LHS in (1) and factor. In (2) we relate the LHS from (1) with the inductive hypothesis, and if the LHS of the IH has an additional $(2+x)$ term, adding that same term to the RHS of the IH will not break the inequality. After factoring in (3), in (4) we show that what we are trying to prove, $2^{(k+1)} + (k+1)2^kx$, is embedded in the RHS along with some additional term. Therefore in (5) we show that if the RHS from (4) with an additional term is less than $(2+x)^{(k+1)}$ then the RHS of (5) without that same additional term must be less than $(2+x)^{(k+1)}$. Thus, because k was arbitrary, we've shown by induction that the inequality holds for any $n \in \mathbb{R}$. \square