6.1200 Problem Set 5

Problem 1

Collaborators: None

Solver: Nathan Leung

Sources Used: None

a) **Proof:**

> Define a pulverizer state machine as described in the problem.

Testing predicate Q on the start state:

$Q(a, b, 1, 0, 0, 1)$

$P_1(a,b)$: $\gcd(a,b) = \gcd(a,b)$ ✓

$P_2(a,1,0)$: $(1)a + (0)b = a$ ✓

$P_3(b,0,1)$: $(0)a + (1)b = b$ ✓

Overall, Q holds for the start state!

> Assume $Q(x, y, s, t, u, v)$ holds true, and initiate a transition to $(x', y', s', t', u', v') = (y, r, u, v, s-qu, t-qv)$

. $P_1(x', y') = P_1(y, r)$

$\gcd(y, r) = \gcd(y, x \bmod y) = \gcd(x, y)$. $\gcd(x,y) = \gcd(a,b)$ from the assumption, so by transitive property of equality P_1 holds true!

. $P_2(x', s', t') = P_2(y, u, v)$ which is $P_3(y, u, v)$ for the old state exactly, so P_2 holds true!

. $P_3(y', u', v') = P_3(r, s-qu, t-qv)$

$(s-qu)a + (t-qv)b = sa + tb - q(ua+vb)$. By $P_2(x, s', t)$, $sa + tb = x$, and by $P_3(y, u, v)$, $ua + vb = y$. Thus $x - qy = (s-qu)a + (t-qv)b = r$,

P_3 holds true!

> P_1, P_2, P_3 of the newly formed state are all satisfied, thus satisfying Q for a state after transition. Thus, Q is proven to be a preserved predicate □

b) Proof :

> Define a pulverizer state machine as described in the problem. By the first step of proof a), Q holds true for the initial state. Additionally by the conclusion of proof a) we conclude that Q is a preserved predicate

> By the invariant principle, Q holds true when the state machine terminates. In the final state $y = 0$, so

$P_1(x, 0) := \gcd(x, 0) = \gcd(a, b)$

$P_2(x, s, t) := sa + tb = x$.

> $\gcd(a, b) = \gcd(x, 0) = x = sa + tb$. Thus we conclude s, t in the final state of the pulverizer satisfies Bézout's identity

c) The pulverizer for variables x, y follow the exact same transition as the Euclidean algorithm state machine $(x, y) \rightarrow (y, x \text{ rem } y)$, so the pulverizer machine should terminate after at most the same number of transitions

Problem 2 -

Collaborators : None

Sources Used : None Solver : Nathan Leung

11 divides 18062, since $18062 = (11)(1642)$. However, 2025 is not divisible by 11 since $2025 \equiv 1 \pmod{11}$. If a and b are arbitrary natural numbers, 11 still divides $18062b$ since $18062b = (11)(1642)(b)$ and from $2025 \equiv 1 \pmod{11}$ we get $2025^a \equiv 1^a \pmod{11}$, $2025^a \equiv 1 \pmod{11}$, $2025^a + 1 \equiv 2 \pmod{11}$, so $2025^a + 1$ is not divisible by 11, and thus cannot be equal to $18062b$! $\square$

Problem 5 -

Collaborators : None

Solver : Nathan Leung

Sources Used : www.wolfphramalpha.com

a) $n = (131394650878384462013)(16257701292567269201)$

via factor n from wolfphramalpha

b) $d \equiv e^{-1} \bmod (p-1)(q-1)$ where p and q are the 2 primes calculated in a

$\equiv 17279741884798386549676652811057029 8307 \pmod{\phi(n)}$

via wolfphram alpha

c) $m \equiv \hat{m}^{d} \pmod{n}$

$\equiv 57734566335007773557714 5663 \pmod{n}$

via wolfphramalpha