CS 173 (B), Spring 2015, Examlet 2, Part A

NAME:	NETID:

Discussion Section: BDA:1PM BDB:2PM BDC:3PM BDD:4PM BDE:5PM

1. For integers a, b, m, define the congruence $a \equiv b \pmod{m}$ in terms of the "divides" relation. (Recall that $x|y$ is said to hold if $\exists z \in \mathbb{Z},\ y = xz$). [2 points]

   Solution: For integers a, b, m, we say $a \equiv b \pmod{m}$ if $m|(a - b)$.

2. Prove that for all positive integers a, b and m, if $a \equiv b \pmod{m}$, then $a^3 \equiv b^3 \pmod{m}$. Use your definition from above. [7 points]

   Solution: Since $a \equiv b \pmod{m}$, we have $m|(a - b)$. So we can let z be an integer such that $(a - b) = zm$, or equivalently, $a = b + zm$. Then,

$$a^3 - b^3 = (b + zm)^3 - b^3 = 3z^2m + 3zm^2 + m^3$$
$$= mw$$

   where $w = 3z^2 + 3zm + m^2$ is an integer. Hence, $m|(a^3 - b^3)$ and by definition, $a^3 \equiv b^3 \pmod{m}$.

   Alternate Solution: Since $a \equiv b \pmod{m}$, we have $m|(a - b)$. So we can let z be an integer such that $(a - b) = zm$. Then,

$$a^3 - b^3 = (a - b)(a^2 + b^2 + ab) = zm(a^2 + b^2 + ab)$$
$$= mw$$

   where $w = z(a^2 + b^2 + ab)$ is an integer. Hence, $m|(a^3 - b^3)$ and by definition, $a^3 \equiv b^3 \pmod{m}$.

3. **Co-primes.** Use the Euclidean algorithm to find two integers x, y such that $9x + 16y = 1$. Show your work. [8 points]

   Solution: Below, $r = \text{remainder}(x, y)$ is the remainder on dividing x by y, $q = \text{quotient}(x, y)$ is quotient.

x	y	r	q	$r = x - q \cdot y$
16	9	7	1	$7 = 16 - 1 \cdot 7$
9	7	2	1	$2 = 9 - 1 \cdot 7$
7	2	1	3	$1 = 7 - 3 \cdot 2$
2	1	0	1	

   From this table we can write:

$$1 = (7 - 3 \times 2)$$
$$= 7 - 3 \times (9 - 7) = 4 \times 7 - 3 \times 9$$
$$= 4 \times (16 - 9) - 3 \times 9 = 4 \times 16 - 7 \times 9$$

   Thus we have $9x + 16y = 1$ for $x = -7$ and $y = 4$.

4. In 1742, Christian Goldbach communicated to Leonhard Euler the following deceptively simple *conjecture*, which remains unproven to this day. [8 points]

Goldbach's Conjecture. Every even integer greater than 2 can be expressed as the sum of two primes.

(a) Write this conjecture as a statement in predicate logic, using the predicates Even and Prime, where the universe is the set of integers $\mathbb{Z}$; you can also use familiar mathematical relations and operators $=, \geq, +$ etc.

Solution:

$$\forall x \in \mathbb{Z}, \exists a, b \in \mathbb{Z} \; \big(\text{Even}(x) \wedge x > 2\big) \rightarrow \big(\text{Prime}(a) \wedge \text{Prime}(b) \wedge (x = a + b)\big)$$

Alternately,

$$\forall x \in \mathbb{Z} \; \big(\text{Even}(x) \wedge x > 2\big) \rightarrow \exists a, b \in \mathbb{Z}\big(\text{Prime}(a) \wedge \text{Prime}(b) \wedge (x = a + b)\big).$$

(b) Then prove this statement, if instead of $\mathbb{Z}$, the universe is restricted to $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. Your proof can use a case analysis (up to 9 cases).

Solution: The statement is vacuously true for $x = 0, 1, 2, 3, 5, 7$. (Optional explanation: for these values of x, the statement $\big(\text{Even}(x) \wedge x > 2\big)$ is false.)
For $x = 4$, pick $a = b = 2$. For $x = 6$, pick $a = b = 3$. For $x = 8$ pick $a = 5, b = 3$. In all these cases, $x = a + b$, and a, b are primes.

CS 173 (B), Spring 2015, Examlet 2, Part A

NAME:	NETID:

Discussion Section: BDA:1PM BDB:2PM BDC:3PM BDD:4PM BDE:5PM

1. For integers a, b, m, define the congruence $a \equiv b \pmod{m}$ in terms of the "divides" relation. (Recall that $x|y$ is said to hold if $\exists z \in \mathbb{Z},\ y = xz$). [2 points]

   Solution: For integers a, b, m, we say $a \equiv b \pmod{m}$ if $m|(a - b)$.

2. Prove that for all positive integers a, b and m, if $a \equiv b \pmod{m}$, then $a^2 - b \equiv b^2 - a \pmod{m}$. Use your definition from above. [7 points]

   Solution: Since $a \equiv b \pmod{m}$, we have $m|(a - b)$. So we can let z be an integer such that $(a - b) = zm$, or equivalently, $a = b + zm$. Then,

$$\begin{aligned}(a^2 - b) - (b^2 - a) &= (b + zm)^2 - b - b^2 + (b + zm) = 2bzm + z^2m^2 + zm \\ &= mw\end{aligned}$$

   where $w = 2bz + z^2m + z$ is an integer. Hence, $m|(a^2 - b^3)$ and by definition, $a^3 \equiv b^3 \pmod{m}$.

   Alternate Solution: Since $a \equiv b \pmod{m}$, we have $m|(a - b)$. So we can let z be an integer such that $(a - b) = zm$. Then,

$$\begin{aligned}(a^2 - b) - (b^2 - a) &= (a^2 - b^2) + (a - b) = (a - b)(a + b + 1) = zm(a + b + 1) \\ &= mw\end{aligned}$$

   where $w = z(a+b+1)$ is an integer. Hence, $m|((a^2 - b) - (b^2 - a))$ and by definition, $a^2 - b \equiv b^2 - a \pmod{m}$.

3. **Co-primes.** Use the Euclidean algorithm to find two integers x, y such that $17x + 23y = 1$. Show your work. [8 points]

   Solution: Below, $r = \text{remainder}(x, y)$ is the remainder on dividing x by y, $q = \text{quotient}(x, y)$ is quotient.

x	y	r	q	$r = x - q \cdot y$
23	17	6	1	$6 = 23 - 1 \cdot 17$
17	6	5	2	$5 = 17 - 2 \cdot 6$
6	5	1	1	$1 = 6 - 1 \cdot 5$
1	1	0	1	

   From this table we can write:

$$\begin{aligned}1 &= 6 - 5 \\ &= 6 - (17 - 2 \times 6) = 3 \times 6 - 17 \\ &= 3 \times (23 - 17) - 17 = 3 \times 23 - 4 \times 17\end{aligned}$$

   Thus we have $17x + 23y = 1$ for $x = -4$ and $y = 3$.

4. In 1742, Christian Goldbach communicated to Leonhard Euler the following deceptively simple *conjecture*, which remains unproven to this day. [8 points]

Goldbach's Conjecture. Every even integer greater than 2 can be expressed as the sum of two primes.

(a) Write this conjecture as a statement in predicate logic, using the predicates Even and Prime, where the universe is the set of integers $\mathbb{Z}$; you can also use familiar mathematical relations and operators $=, \geq, +$ etc.

Solution:

$$\forall x \in \mathbb{Z}, \exists a, b \in \mathbb{Z}\ \big(\text{Even}(x) \land x > 2\big) \rightarrow \big(\text{Prime}(a) \land \text{Prime}(b) \land (x = a + b)\big)$$

Alternately,

$$\forall x \in \mathbb{Z}\ \big(\text{Even}(x) \land x > 2\big) \rightarrow \exists a, b \in \mathbb{Z}\big(\text{Prime}(a) \land \text{Prime}(b) \land (x = a + b)\big).$$

(b) Then prove this statement, if instead of $\mathbb{Z}$, the universe is restricted to $\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$. Your proof can use a case analysis (up to 9 cases).

Solution: The statement is vacuously true for $x = 0, 1, 2, 3, 5, 7$. (Optional explanation: for these values of x, the statement $\big(\text{Even}(x) \land x > 2\big)$ is false.)
For $x = 4$, pick $a = b = 2$. For $x = 6$, pick $a = b = 3$. For $x = 8$ pick $a = 5, b = 3$. In all these cases, $x = a + b$, and a, b are primes.