

M417 Exam 1 Solutions**March 1, 2004**

(1) Give an example of a set S and a binary operation $*$: $S \times S \rightarrow S$ that is not associative.

Solution: Let S be the set of positive rational numbers, and define $a * b = a/b$. Then $2 * (3 * 4) = 2/(3/4) = 8/3 \neq 1/6 = (2/3)/4 = (2 * 3) * 4$.

(2) Find the inverse of 5 in $U(323)$; i.e., find the decryption exponent d , given $e = 5$ and $n = 17 * 19$. Note that $323 = 17 * 19$.

Solution: We need to find a positive integer d such that $5d \pmod{323} = 1$. We can use the Euclidean algorithm: $323 = 5(64) + 3$ (hence $1(323) - 64(5) = 3$), $5 = 3(1) + 2$ (hence $1(5) - [1(323) - 64(5)] = 2$ or $-1(323) + 65(5) = 2$), $3 = 2(1) + 1$ (hence $1(3) - 1(2) = 1$, or $1(1(323) - 64(5)) - 1(-1(323) + 65(5)) = 1$, so $2(323) - 129(5) = 1$ and thus $(2-5)(323) + (323-129)(5) = 1$). Thus $d = 323 - 129 = 194$.

(3) Use induction to prove that $2 + 4 + \cdots + 2n = n^2 + n$.

Solution: First, we check the formula for $n = 1$: $2 = 1^2 + 1$. Then we assume the formula for $1 \leq k < n$. Thus $2 + 4 + \cdots + 2n = (2 + 4 + \cdots + 2(n-1)) + 2n = ((n-1)^2 + (n-1)) + 2n = (n^2 - n) + 2n = n^2 + n$. This proves the result for all $n \geq 1$.

(4) If $f: A \rightarrow B$ is a surjective function, show that $f^{-1}: 2^B \rightarrow 2^A$ is injective.

Solution: See the solutions to Homework 5.

(5) Consider $g = 8100 \in \mathbf{Z}_{17280}$. Recall that $1728 = 12^3$. Find $|g|$, and find the largest positive integer $m < 17280$ such that $\langle m \rangle = \langle g \rangle$.

Solution: First, using prime factorization, we see $\gcd(8100, 17280) = \gcd(2^2 * 3^4 * 5^2, 2^7 * 3^3 * 5) = 2^2 * 3^3 * 5 = 540$. Thus $\langle 8100 \rangle = \langle 540 \rangle$, and $|8100| = |540| = 17280/540 = 2^5 = 32$. Also, $31 * 540 = 17280 - 540 = 16740$ is the largest element of $\langle 540 \rangle$, yet $|16740| = 17280/\gcd(17280, 16740) = 32$ (alternatively, 16740 is the inverse of 540, so has the same order as 540), so $\langle 16740 \rangle = \langle 8100 \rangle$.

(6) Let a and b be elements of a group G . Show that $|ab| = |ba|$.

Solution: If $|ab| = n < \infty$, then $(ab)^n = e$. Hence $ba = b(ab)^n a = (ba)^{n+1}$, so $e = (ba)^n$, and we have $|ba| \leq |ab|$. Switching the roles of a and b now gives $|ab| \leq |ba|$, and hence $|ba| = |ab|$. Thus if one has finite order, then so does the other, and the orders are equal. If one has infinite order, then so must the other (since whenever either one has finite order so does the other), and hence again the orders are equal.

M417 Exam 1 Solutions**March 1, 2004**

(1) Give an example of a set S and a binary operation $*$: $S \times S \rightarrow S$ that is not associative.

Solution: Let S be the set of positive rational numbers, and define $a * b = a/b$. Then $2 * (3 * 4) = 2/(3/4) = 8/3 \neq 1/6 = (2/3)/4 = (2 * 3) * 4$.

(2) Find the inverse of 5 in $U(323)$; i.e., find the decryption exponent d , given $e = 5$ and $n = 17 * 19$. Note that $323 = 17 * 19$.

Solution: We need to find a positive integer d such that $5d \pmod{323} = 1$. We can use the Euclidean algorithm: $323 = 5(64) + 3$ (hence $1(323) - 64(5) = 3$), $5 = 3(1) + 2$ (hence $1(5) - [1(323) - 64(5)] = 2$ or $-1(323) + 65(5) = 2$), $3 = 2(1) + 1$ (hence $1(3) - 1(2) = 1$, or $1(1(323) - 64(5)) - 1(-1(323) + 65(5)) = 1$, so $2(323) - 129(5) = 1$ and thus $(2-5)(323) + (323-129)(5) = 1$). Thus $d = 323 - 129 = 194$.

(3) Use induction to prove that $2 + 4 + \cdots + 2n = n^2 + n$.

Solution: First, we check the formula for $n = 1$: $2 = 1^2 + 1$. Then we assume the formula for $1 \leq k < n$. Thus $2 + 4 + \cdots + 2n = (2 + 4 + \cdots + 2(n-1)) + 2n = ((n-1)^2 + (n-1)) + 2n = (n^2 - n) + 2n = n^2 + n$. This proves the result for all $n \geq 1$.

(4) If $f: A \rightarrow B$ is a surjective function, show that $f^{-1}: 2^B \rightarrow 2^A$ is injective.

Solution: See the solutions to Homework 5.

(5) Consider $g = 8100 \in \mathbf{Z}_{17280}$. Recall that $1728 = 12^3$. Find $|g|$, and find the largest positive integer $m < 17280$ such that $\langle m \rangle = \langle g \rangle$.

Solution: First, using prime factorization, we see $\gcd(8100, 17280) = \gcd(2^2 * 3^4 * 5^2, 2^7 * 3^3 * 5) = 2^2 * 3^3 * 5 = 540$. Thus $\langle 8100 \rangle = \langle 540 \rangle$, and $|8100| = |540| = 17280/540 = 2^5 = 32$. Also, $31 * 540 = 17280 - 540 = 16740$ is the largest element of $\langle 540 \rangle$, yet $|16740| = 17280/\gcd(17280, 16740) = 32$ (alternatively, 16740 is the inverse of 540, so has the same order as 540), so $\langle 16740 \rangle = \langle 8100 \rangle$.

(6) Let a and b be elements of a group G . Show that $|ab| = |ba|$.

Solution: If $|ab| = n < \infty$, then $(ab)^n = e$. Hence $ba = b(ab)^n a = (ba)^{n+1}$, so $e = (ba)^n$, and we have $|ba| \leq |ab|$. Switching the roles of a and b now gives $|ab| \leq |ba|$, and hence $|ba| = |ab|$. Thus if one has finite order, then so does the other, and the orders are equal. If one has infinite order, then so must the other (since whenever either one has finite order so does the other), and hence again the orders are equal.