Modular Arithmetic Practice, Math 150

Solutions will not be provided to these sheets. If you wish to talk through these problems, either attend the study halls or come to office hours.

The Division Algorithm: $n = qd + r$, $n, q, d, r \in \mathbb{Z}$, $0 \leq r \leq d - 1$.
For each of the following pairs of values for n and d, find q and r as in the division algorithm.

- $n = 100, d = 9$
- $n = 4925, d = 7$
- $n = 2113, d = 306$
- $n = 32768, d = 41$

The mod and div functions: If $n = qd + r$ as in the division algorithm, then $q = n \text{ div } d$ and $r = n \bmod d$.
For each of the following, d, n div d, and n mod d will be given. Find n. If the given values are not possible, explain why.

- n div $4 = 3$, n mod $4 = 3$
- n div $12 = -16$, n mod $12 = 0$
- n div $7 = 21$, n mod $7 = 5$
- n div $8 = 901$, n mod $8 = 8$.

The Divisibility Relation: For $n, m \in \mathbb{Z}$, $n|m$ if $\exists k \in \mathbb{Z}$ so that $nk = m$.
For each pair of n, m, determine whether or not $n|m$

- $n = 3, m = 913$
- $n = 17, m = 731$
- $n = 2, m = -684$
- $n = -6, m = 84$
- $n = 12, m = 200$
- $n = 0, m = 1040$
- $n = 210, m = 3$
- $n = 47, m = 0$

Congruence Relations: For $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, we say $a \equiv b \pmod{m}$ if $m|(a - b)$.
For each a, b, m given, determine if $a \equiv b \pmod{m}$.

- $a = 1, b = 47, m = 23$
- $a = 203, b = 600, m = 3$
- $a = 0, b = 1002, m = 11$
- $a = 1768, b = -6, m = 13$

For each a, m given, determine the smallest non-negative integer b such that $a \equiv b \pmod{m}$.

- $a = 14, m = 2$
- $a = 271, m = 13$
- $a = 16, m = 94$
- $a = 275, m = 16$

Find the smallest non-negative integer congruent to the given expression modulo the given m.

- $23 + 31 \equiv ? \pmod{7}$
- $-12 + 101^6 \equiv ? \pmod{25}$
- $27 \cdot (-3) \cdot (14 + 51) \equiv ? \pmod{11}$
- $41 - 16 \cdot 3 \equiv ? \pmod{20}$
- $3 \cdot 5 \cdot 7 \cdot 100 \equiv ? \pmod{73}$
- $(31 + 26) \cdot (25 - 42) \equiv ? \pmod{17}$

Base b Expansions: Let $b > 1$ an integer and $n \in \mathbb{N}$. The base b representation of n is, with $0 \leq a_i \leq b - 1$ for all i and $a_m \neq 0$

$$n = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_1 b^1 + a_0.$$

We write $n = (a_m a_{m-1} \ldots a_1 a_0)_b$.
In the following, you will be given a number n written in some base and a value $b > 1$. Write n in base b.

- $n = 210, b = 2$
- $n = (AA3)_{16}, b = 10$
- $n = (10110111010)_2, b = 10$
- $n = 3251, b = 8$
- $n = (F3C)_{16}, b = 2$
- $n = (537)_8, b = 10$
- $n = (216)_8, b = 2$
- $n = (10001010101)_2, b = 16$
- $n = (100100111)_2, b = 8$

Modular Exponentiation: A particularly fast algorithm to compute $a^n \bmod m$.
For each of the following a, n, m are given. Apply the modular exponentiation algorithm.

- $a = 21, n = 3, m = 35$
- $a = 7, n = 17, m = 19$
- $a = 2, n = 298, m = 23$
- $a = 50, n = 481, m = 7$
- $a = 611, n = 100, m = 11$
- $a = -2, n = 25, m = 33$

Prime Factorization: Every positive integer can be written uniquely as a product of prime numbers in decreasing order.
For each of the following integers, find its prime factorization. You may find the following list of small primes helpful:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, \ldots$$

- 211
- 63
- 5247
- 113
- 574

Greatest Common Divisors & Euclidean Algorithm: The key lemma for the Euclidean algorithm is that if $a = bq+r$ (all integers), then $\gcd(a, b) = \gcd(b, r)$.
Use the Euclidean algorithm to find the gcd of each pair of integers.

- 213, 97
- 4315, 85
- 6234, 426
- 123, 691
- 351, 7182
- 2700, 131

Bezout Coefficients: If $a, b \in \mathbb{N}$, then $\exists s, t \in \mathbb{Z}$ such that $sa + tb = \gcd(a, b)$. s, t are *Bezout coefficients.*
Use the reversed Euclidean algorithm strategy to find Bezout coefficients for the given pair of integers.

- 213, 97
- 1111, 111
- 67, 43
- 5247, 106

Finding Inverses Modulo m: If $\gcd(a, m) = 1$, find the inverse of a modulo m by finding Bezout coefficients for a, m, the coefficient of a is the inverse modulo m.
For each of the following a, m find the inverse of a modulo m, write it as the smallest possible non-negative integer mod m congruent to your result.

- $a = 97, m = 213$
- $a = 16, m = 45$
- $a = 100, m = 7$

Solving Linear Congruences: To solve $ax \equiv b \pmod{m}$ for x if $\gcd(a, m) = 1$, multiply both sides by the inverse of a modulo m.
For each of the following equations, solve for x, in smallest non-negative form.

- $3x \equiv 5 \pmod{7}$
- $21x \equiv 7 \pmod{25}$
- $-2x \equiv 4 \pmod{31}$
- $16x \equiv 11 \pmod{101}$
- $7x \equiv 31 \pmod{97}$
- $11x \equiv 92 \pmod{314}$