MATH 363 Discrete Mathematics
Assignment 5

Due by February 17th

1. (**2pt**)Prove or disprove that if $a|c$ and $b|d$, then $ab|cd$.
2. (**2pt**) Prove or disprove that $a|bc$ implies that either $a|b$ or $a|c$.
3. (**2pt**) Decode the following message encripted with Caesar's cipher: **Darorwv olyh lq Arfklplofr.**
4. (**3pt**) Let $a, m \in \mathbf{Z}$ and $m > 0$. Find a formula for the integer with smallest absolute value that is conruent to a $(\mathbf{mod}\ m)$.
5. (**2pt**) Consider the linear congruence generated by $x_{n+1} = 2x_n(\mathbf{mod}\ 18)$ with seed $x_0 = 17$. How many pseudorandom numbers can we generate before numbers start repeating?
6. (**3pt**) Prove that there are infinitely many prime numbers.
7. (**1pt each**) Find the following values and express them as product of prime numbers
   i) $gcd(18, 99)$
   ii) $lcm(18, 99)$
   iii) $gcd(2^3 \cdot 3 \cdot 5^2, 2 \cdot 7 \cdot 5^4)$
   iv) $lcm(2^3 \cdot 3 \cdot 5^2, 2 \cdot 7 \cdot 5^4)$
8. (**3pt**) Prove or disprove that for any positive integers a, b,
$$a \cdot b = gcd(a, b) \cdot lcm(a, b)$$
9. (**2pt each**) Find the inverse of the following numbers
   i) $2(\mathbf{mod}\ 17)$
   ii) $3(\mathbf{mod}\ 18)$
10. (**2pt**) Solve the congruence $2x - 5 = 3(\mathbf{mod}\ 17)$
11. (**3pt**) Show that $10! = -1(\mathbf{mod}\ 11)$ without explicitly computing $10!$. (Hint: Pair the factors of $10!$ using the inverse of $a(\mathbf{mod}\ 11)$ for $1 \leq a \leq 10$.)
12. (**2pt**) Find $5^{268}(\mathbf{mod}\ 7)$ using modular exponentiation.
13. (**2pt each**) What is the smallest positive integer that can be written as a linear combination of (justify your answer)
   i) 5 and 7
   ii) 4 and 22
14. (**4pt**) What is the original message encrypted using the RSA system with $n = 53 \cdot 61$ and $e = 17$ if the encrypted message is 3185203824602550? (To decrypt, first verify that the decryption exponent is $d = 2753 = (17)^{-1}(\bmod 52 \cdot 60)$.)

Extra:3pt Prove using the Euclidean algorithm that $1 = 2(52 \cdot 60) - 17 \cdot 367 = -15(52 \cdot 60) + 17 \cdot 2753$.

15. (**2pt**) Let $A = \begin{pmatrix} a_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k \end{pmatrix}$ be an $k \times k$ diagonal matrix. Show that for any $n \in \mathbf{N}$,

$$A^n = \begin{pmatrix} a_1^n & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & a_k^n \end{pmatrix}$$