Math 471 - Practice Final Exam

Problem 1. Recall that for integers a, b we say that $a < b$ if $b + -a \in \mathbf{Z}^+$. Give a careful proof (from the axioms) of the following statement:

If $a, b \in \mathbf{Z}$, $c \in \mathbf{Z}^+$, and $a < b$, then $ac < bc$.

Problem 2. Find all positive integers n such that $12|n$ and $n|816$.

Problem 3. Find all solutions to

$$11x + 17y = 305$$

with $x, y \in \mathbf{Z}^+$.

Problem 4. Compute $31^{1209} \bmod 101$. (Hint: first use Fermat's little theorem to reduce the exponent.)

Problem 5. Find an $x \in \mathbf{Z}$ such that

$$x \equiv 2 \pmod{10};$$
$$x \equiv 7 \pmod{11}.$$

Problem 6. How many roots does the polynomial $f(x) = x^8 - 1$ have in $\mathbf{Z}/91$?

Problem 7. Below is a table of logarithms for $(\mathbf{Z}/17)^\times$ with respect to the primitive root $g = 3$:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\log_3 a$	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Use the table to find all $x \in \mathbf{Z}/17$ such that

$$x^{12} \equiv 13 \pmod{17}.$$

Problem 8. Is 198 a square modulo the prime 223?

Problem 9. Consider the RSA code with $n = 187$ and $e = 23$. (So a message x is encrypted by computing $x^{23} \bmod 187$.) Decode the encrypted message `144`.

Problem 10. How many zeros does 62! end in?

Problem 11. Find the general solution to the linear diophantine equation

$$17x + 31y = 3.$$

Problem 12. Fix an integer n and an element $a \in \mathbf{Z}/n$. Let e denote the order of a. Prove that the order of a^2 is either e or $e/2$ depending on whether e is odd or even.

Problem 13.

((a)) Use the Chinese remainder theorem to find an integer x such that

$$x \equiv 4 \pmod{7}$$
$$x \equiv 10 \pmod{13}.$$

((b)) Does there exist an integer x such that

$$x \equiv 11 \pmod{12}$$
$$x \equiv 5 \pmod{14}$$
$$x \equiv 19 \pmod{21}?$$

Why or why not? (You need not exhibit such an x if it exists.)

Problem 14. Find the largest two digit prime number p such that -5 is a square mod p. (Hint: the simplest way is to figure out for which p you have $\left(\frac{-5}{p}\right) = 1$.)