MATH 471 - PRACTICE EXAM 2

Problem 1.

(a) Compute $\frac{1}{11}$ in $\mathbf{Z}/17$.
(b) Compute $\frac{7}{11}$ in $\mathbf{Z}/17$.

Problem 2. Compute 31^{1209} mod 101. (Hint: first use Fermat's little theorem to reduce the exponent.)

Problem 3. Consider the RSA code with $n = 187$ and $e = 23$. (So a message x is encrypted by computing x^{23} mod 187.) Decode the encrypted message `144`.

Problem 4. How many zeros does 62! end in?

Problem 5. (5 points each) Find all solutions of the congruences below.

(1) $8x \equiv 7 \pmod{11}$
(2) $36x \equiv 18 \pmod{60}$
(3) $5x \equiv 15 \pmod{25}$

Problem 6. For each of the following expressions, give all elements matching the given description or explain why none exist.

(a) $\frac{1}{5} \in \mathbf{Z}/13$
(b) $\frac{3}{7} \in \mathbf{Z}/14$
(c) $\sqrt{5} \in \mathbf{Z}/11$
(d) $\sqrt{-1} \in \mathbf{Z}/11$
(e) $\sqrt[3]{2} \in \mathbf{Z}/5$

Problem 7. Find all solutions of each linear congruence below.

(a) $3x \equiv 7 \pmod{13}$
(b) $4x \equiv 10 \pmod{14}$
(c) $5x \equiv 13 \pmod{15}$

Problem 8. Consider the RSA code with $n = 187$ and $d = 107$. (That is, a message X is encoded to X^{107} modulo 187.) Break this code and decode the recieved message $Y = 10$ using the following data in $\mathbf{Z}/187$:

$$10^2 = 100, 10^4 = 89, 10^8 = 67, 10^{16} = 1, 100^{32} = 1, 100^{64} = 1, 10^{128} = 1.$$