Name: ______________________________ Score (Out of 12 points):

A non-programmable, non-scientific calculator may be used.

1. [3 points] Use the quadratic sieve method to factor $n = 713$. You may find the following helpful:

$$47^2 \equiv 70 \equiv (2)(5)(7) \pmod{713}$$
$$60^2 \equiv 35 \equiv (5)(7) \pmod{713}$$
$$71^2 \equiv 50 \equiv (2)(5^2) \pmod{713}$$

2. [3 points] Use the "Baby step, Giant step" method to find all solutions to $3^x \equiv 59 \pmod{89}$, noting that 3 is a primitive root of the prime 89. You may find the following helpful:

$$59 \cdot 3^{(0)(10)} \equiv 59 \pmod{89}$$
$$59 \cdot 3^{-(1)(10)} \equiv 12 \pmod{89}$$
$$59 \cdot 3^{-(2)(10)} \equiv 13 \pmod{89}$$
$$59 \cdot 3^{-(3)(10)} \equiv 66 \pmod{89}$$
$$59 \cdot 3^{-(4)(10)} \equiv 27 \pmod{89}$$
$$59 \cdot 3^{-(5)(10)} \equiv 7 \pmod{89}$$

The quiz continues on the back of the page.

3. Below are a list of q-ary codes. For each code, determine q, the type (n, M, d), and the code rate R.

   (a) [2 points] Let $\mathcal{A} = \{0, 1\}$, and let $C \subseteq \mathcal{A}^n$ be the code

$$C = \{(0,0,0), (0,1,1), (1,0,1), (1,1,0)\}.$$

   (b) [2 points] Let $\mathcal{A} = \{0, 1, 2\}$, and let C be the ternary repetition code

$$C = \{(0,0,0,0), (1,1,1,1), (2,2,2,2)\}.$$

   (c) [2 points] Let $\mathcal{A} = \{0, 1, 2, 3, 4\}$, and define a code as follows: Given a 5-letter word in $\mathcal{A}$, say, $(a_1, a_2, a_3, a_4, a_5)$, add a 6^{th} digit $a_6 \in \mathcal{A}$ so that

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 \equiv 0 \pmod 5.$$