Name: ______________________________ Score (Out of 12 points):

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

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

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

If we take the product of all three of the numbers, we find:

$$(47 \cdot 60 \cdot 71)^2 \equiv 2^2 \cdot 5^4 \cdot 7^2 \equiv (2 \cdot 5^2 \cdot 7)^2 \pmod{713} \qquad \text{and so}$$

$$(47 \cdot 60 \cdot 71) \equiv 200\,220 \equiv 580 \pmod{713} \qquad \text{and} \qquad (2 \cdot 5^2 \cdot 7) \equiv 350 \pmod{713}$$

are both square roots of the same number, and $\gcd(580-350, 713) = \gcd(230, 713)$ should yield a factor of 713. We use the Euclidean algorithm to compute the gcd:

$$713 = 3(230) + 23$$
$$230 = 10(23)$$

We conclude that $\gcd(230, 713) = 23$, and 23 is a factor of 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:

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

We recognize the $(59)3^{-(4)(10)} \equiv 27 \pmod{89}$ as a power of 3, and so

$$59 \cdot 3^{-(4)(10)} \equiv 3^3 \pmod{89}$$
$$59 \equiv 3^3 \cdot 3^{40} \pmod{89}$$
$$59 \equiv 3^{43} \pmod{89}$$

and so we find that $x = 43$ is a solution. Since 3 is a primitive root of 89, the set of all solutions is precisely the congruence class of 43 modulo $(89 - 1) = 88$.

 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

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

Here $q = |\mathcal{A}| = 2$, and the length of the codewords is $n = 3$. The number of codewords is $M = 4$. By inspection, all codewords differ from each other in two coordinates, so $d = 2$. (It is, in fact, the subspace of $(\mathbb{Z}/2\mathbb{Z})^3$ with digit-sum of 0 modulo 2).

The code rate is $R = \dfrac{\log_q(M)}{n} = \dfrac{\log_2(4)}{3} = \dfrac{2}{3}$.

We have a $(3, 4, 2)$ code with code rate $R = \frac{2}{3}$.

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

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

Here $q = 3$, and the length of the codewords is $n = 4$. The number of codewords is $M = 3$. All codewords differ from each other in all four coordinates, so $d = 4$. This is the length-4 ternary repetition code.

The code rate is $R = \dfrac{\log_q(M)}{n} = \dfrac{\log_3(3)}{4} = \dfrac{1}{4}$.

We have a $(4, 3, 4)$ code with code rate $R = \frac{1}{4}$.

(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

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

Here $q = 5$, and the length of the codewords is $n = 6$. The number of codewords is $M = 5^5$, since every codeword is determined by its first 5 coordinates, and any choice of first 5 coordinates gives a valid codeword.

Any two codewords must differ in at least two coordinates, since changing a single coordinate of a codeword would violate the sum-zero condition. It is, however, possible to change only 2 coordinates in a codeword and obtain a new valid codeword, so $d = 2$.

The code rate is $R = \dfrac{\log_q(M)}{n} = \dfrac{\log_5(5^5)}{6} = \dfrac{5}{6}$.

We have a $(6, 5^5, 2)$ code with code rate $R = \frac{5}{6}$.