Math373 **Quiz 12** **Fri. Apr 22, 2022**

Name: ____________________

Directions: Show all work. No credit for answers without work.

1. Let $p = 41$. Alice and Bob use Elliptic Curve Diffie-Hellman to exchange a secret. They agree to use $E\colon\ y^2 = x^3 + 19x + 20$ over $\mathbb{F}_p$ with base point $g = (2, 5)$. The following powers of g are given for convenience.

n	1	2	4	8	16	32
g^n	$(2, 5)$	$(38, 31)$	$(24, 27)$	$(36, 13)$	$(9, 31)$	$(22, 4)$

(a) [**1 point**] Find the base point inverse g^{-1}.

(b) [**3 points**] Alice chooses private exponent $a = 17$. What should she send to Bob?

(c) [**2 points**] Bob chooses private exponent $b = 2$. What is their shared secret?

2. [**4 points**] Let $p = 31$, and let $\mathbf{a} = x^5 - 4x^2 + 1$ and $\mathbf{b} = x^2 + 1$ be polynomials in $\mathbb{F}_p[x]$. Find $\mathbf{q}$ and $\mathbf{r}$ such that $\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r}$ with $\mathbf{r} = 0$ or $\deg(\mathbf{r}) < \deg(\mathbf{b})$. In your final answer, normalize all coefficients to values in the set $\{0, \ldots, p-1\}$.