Name: Solutions

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}.

$g^{-1} = \boxed{(2,-5)}$ since $(2,5)(2,-5) = \mathcal{O}$

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

She sends $A = g^a = g^{16+1} = g^{16} \cdot g^1 = \underbrace{(9,31)}_{P_2} \cdot \underbrace{(2,5)}_{P_1}$

- $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1} = \dfrac{31-5}{9-2} = \dfrac{26}{7} = 26 \cdot 7^{-1} = 26 \cdot 6 = 33.$

- Need 7^{-1} mod 41. $7 \cdot 6 = 42$, so $7^{-1} = 6$.

$x_3 = \lambda^2 - x_1 - x_2 = (33)^2 - 2 - 9 = 23 - 11 = 12$

$y_3 = \lambda(x_1 - x_3) - y_1 = 33(2-12) - 5 = -335 = 34.$ So $\boxed{A = (12,34)}$

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

We need $g^{ab} = (g^a)^b = A^b = (12,34) \cdot (12,34)$

$y^2 = x^3 + Ax + B$
$2yy' = 3x^2 + A$, $\lambda = y' = \dfrac{3x^2+A}{2y}$

$\lambda = \dfrac{3x_1^2 + A}{2y_1} = \dfrac{3(12)^2 + 19}{2(34)} = \dfrac{451}{68} = \dfrac{0}{68} = 0$

$x_3 = \lambda^2 - x_1 - x_2 = 0 - 12 - 12 = -24 = 17$

$y_3 = \lambda(x_1 - x_3) - y_1 = 0(\sim) - 34 = -34 = 7$

So shared secret is $A^b = \boxed{(17,7)}$.

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 $\{0, \ldots, p-1\}$.

$$
\begin{array}{r|l}
 & x^3 \qquad\qquad - x \;\; - 4 \\
\hline
x^2 + 1 & x^5 + 0x^4 + 0x^3 - 4x^2 + 0x + 1 \\
 & x^5 \qquad + x^3 \\
\hline
 & \qquad -x^3 - 4x^2 + 0x + 1 \\
 & \qquad -x^3 \qquad\;\; - x \\
\hline
 & \qquad\qquad -4x^2 + x + 1 \\
 & \qquad\qquad -4x^2 \qquad - 4 \\
\hline
 & \qquad\qquad\qquad\quad x + 5
\end{array}
$$

So $\underbrace{x^5 - 4x^2 + 1}_{a} = \underbrace{(x^3 - x - 4)}_{q}\underbrace{(x^2+1)}_{b} + \underbrace{(x+5)}_{r}$

Take $q = x^3 - x - 4 = \boxed{x^3 + 30x + 27}$ [normalize coefficients]

$\boxed{r = x+5}$