Rows 1 and 5 are dependent and lead to the factorization $661 \cdot 1511$.

§ **VI.1.**

1. Either the circle group (if the real curve has one connected component) or the product of the circle group and the two-element group (if it has two connected components). An example of the first is $y^2 = x^3 + x$; an example of the second is $y^2 = x^3 - x$ (for an equation of the form (1), this depends on whether the cubic on the right has 1 or 3 real roots).
2. n^2 complex points of order n; n real points of order n if n is odd, and either n or $2n$ if n is even, depending on whether the real curve has one or two components.
3. Same examples as in Exercise 1.
4. (a) On the x-axis; (b) inflection point; (c) a point where a line from an x-intercept of the curve is tangent to the curve (in addition to the points in (a)).
5. (a) 3; (b) 4; (c) 7; (d) 5.
6. Characteristic 2: $x_3 = \frac{y_1^2+y_2^2}{x_1^2+x_2^2}+x_1+x_2$, $y_3 = c+y_1+\frac{y_1+y_2}{x_1+x_2}(x_1+x_3)$, and when $P = Q$ we have $x_3 = \frac{x_1^4+a^2}{c^2}$, $y_3 = c+y_1+\frac{x_1^2+a}{c}(x_1+x_3)$; and for equation (2b): $x_3 = \frac{y_1^2+y_2^2}{x_1^2+x_2^2} + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a$, $y_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + x_3 + y_1$, and when $P = Q$ we have $x_3 = x_1^2 + \frac{b}{x_1^2}$, $y_3 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3$; characteristic 3: $x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - a - x_1 - x_2$, $y_3 = -y_1+\frac{y_2-y_1}{x_2-x_1}(x_1-x_3)$, and when $P = Q$ we have $x_3 = \left(\frac{ax_1-b}{y_1}\right)^2 - a+x_1$, $y_3 = -y_1 + \frac{ax_1-b}{y_1}(x_1 - x_3)$.
7. (a) Show that in each pair $\{a, -a\}$ exactly one of the values $x = \pm a$ leads to 2 solutions (x, y) to the equation (treat $x = 0$ and the point at infinity separately). (b)–(c) Use the fact that $x \mapsto x^3$ is a 1-to-1 map of $\mathbf{F}_q$ to itself when $q \equiv 2 \mod 3$.
8. The following table shows the type of the abelian group for each value of q and each of the two elliptic curves:

q	3	5	7	9	11	13	17
$y^2 = x^3 - x$	(2, 2)	(4, 2)	(4, 2)	(4, 4)	(2, 2, 3)	(4, 2)	(4, 4)
$y^2 = x^3 - 1$	––	(2, 3)	(2, 2)	––	(4, 3)	(2, 2, 3)	(2, 9)

19	23	25	27
(2, 2, 5)	(4, 2, 3)	(8, 4)	(2, 2, 7)
(2, 2, 7)	(8, 3)	(2, 2, 3, 3)	––

9. (a) Let $P = (x, y)$. Then $-P = (x, y + 1)$, $2P = (x^4, y^4 + 1)$. (b) We have $2(2P) = (x^{16}, y^{16} + 1 + 1) = (x^{16}, y^{16}) = (x, y) = P$. (c) By part (b), $2P = -P$, i.e., $(x^4, y^4+1) = (x, y+1)$; but this means that $x^4 = x$ and $y^4 = y$, so that x and y are in the field of 4 elements. By Hasse's theorem, the number N of points is within $2\sqrt{4} = 4$ of $4+1$ and within $2\sqrt{16} = 8$ of $16 + 1$, i.e., $N = 9$.