P1. Recall that an Azumaya algebra over a field $k$ is a twist of a matrix algebra, i.e., a $k$-algebra $A$ (associative with 1) such that $A \otimes_k k^{\text{sep}} \cong M_n(k^{\text{sep}})$ for some $n \in \mathbb{Z}_{>0}$. Let $A, B$ be Azumaya $k$-algebras. Prove that:

(a) The tensor product $A \otimes_k B$ is an Azumaya $k$-algebra.
(b) The opposite algebra $A^{\text{op}}$ is an Azumaya algebra.
(c) The map $A \otimes_k A^{\text{op}} \to \text{End}_k A$ sending $a \otimes b$ to the $k$-linear map $x \mapsto axb$ is a $k$-algebra isomorphism. (Here $\text{End}_k A$ is the $k$-algebra of $k$-linear endomorphisms of $A$ viewed as a $k$-vector space, so $\text{End}_k A$ is isomorphic to a matrix algebra.)
(d) For any field extension $L$ of $k$, the $L$-algebra $A \otimes_k L$ is an Azumaya $L$-algebra.
(e) $A$ is central (i.e., its center is $k$).
(f) $A$ is simple (i.e., it has exactly two 2-sided ideals, namely $(0)$ and $A$ itself).

P2. How many different proofs can you find for the statement that for $a, b \in \mathbb{F}_q^\times$ with $q$ odd, the quadratic form $x^2 - ay^2 - bz^2$ has a nontrivial zero? (Actually, it is trivially true for even $q$ too.)

P3. Using the previous exercise, prove that if $k$ is a nonarchimedean local field with (finite) residue field of odd size, and $a, b \in k$ are units (elements of valuation 0), then the quaternion algebra $(a, b)$ over $k$ is split.

P4. Describe a method for computing $\text{inv}_p(a, b) \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}$ for any $a, b \in \mathbb{Q}^\times$ and for any $p \leq \infty$.

P5. Let $p$ and $q$ be odd primes. The reciprocity law for the Brauer group, i.e., the exactness of

$$0 \to \text{Br} \mathbb{Q} \to \bigoplus_v \text{Br} \mathbb{Q}_v \to \mathbb{Q}/\mathbb{Z} \to 0,$$

implies that

(*) the number of places at which the quaternion algebra $(p, q)$ ramifies is even.

Show that (*) is equivalent to quadratic reciprocity for $p$ and $q$.

P6. Use the reciprocity law for the Brauer group to prove the Legendre symbol formula

$$(\frac{2}{p}) = \begin{cases} +1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

P7. Let $\{K_\alpha\}$ be a directed system of fields, and let $K = \varinjlim K_\alpha$ be the direct limit. Prove that $\text{Br} K = \varprojlim \text{Br} K_\alpha$.

P8. (a) Let $k$ be a global field, and let $a \in \text{Br} k$. Prove that there is a root of unity $\zeta \in \overline{k}$ such that the image of $a$ in $\text{Br} k(\zeta)$ is 0.
(b) Let $k$ be a global field, and let $k^{ab}$ denote its maximal abelian extension. Prove that $\text{Br} k^{ab} = 0$.
P9. Let $X$ be a $k$-variety. Explain why the map $\mathrm{Br}\, k \to \mathrm{Br}\, X$ is injective when $X$ has a $k$-point, or when $k$ is a global field and $X(A) \neq \emptyset$.

P10. Let $k$ be a field of characteristic 0. Let $X$ be a smooth plane conic in $\mathbb{P}^2$. Since $X$ is a twist of $\mathbb{P}^1$, it corresponds to an element of $H^1(k, \text{Aut}\, \mathbb{P}^1_{k_{\text{sep}}}) = H^1(k, \text{PGL}_2)$, and hence gives an element $\alpha \in \mathrm{Br}\, X$ of order dividing 2. Prove that $\mathrm{Br}\, k \to \mathrm{Br}\, X$ is surjective, and that its kernel is generated by $\alpha$.

P11. (Iskovskikh’s counterexample to the local-global principle)
(a) Construct a smooth projective model $X$ of the affine variety
\[ X_0: y^2 + z^2 = (x^2 - 2)(3 - x^2) \]
over $\mathbb{Q}$. (Suggestion: extend $x: X_0 \to \mathbb{A}^1$ to a morphism $X \to \mathbb{P}^1$ with $X$ a closed subscheme of a $\mathbb{P}^2$-bundle over $\mathbb{P}^1$ such that each geometric fiber of $X \to \mathbb{P}^1$ is either a smooth plane conic or a union of two distinct lines.)
(b) Prove that $X(A) \neq \emptyset$.
(c) Let $K$ be the function field of $X$. Let $A$ be the class of $(-1, x^2 - 2)$ in $\mathrm{Br}\, K$. Let $B$ be the class of $(-1, 3 - x^2)$ in $\mathrm{Br}\, K$. Let $C$ be the class of $(-1, 1 - 2/x^2)$ in $\mathrm{Br}\, K$. Prove that $A = B = C$.
(d) Prove that $A \in \mathrm{Br}\, X$. (Hints: Equivalently, one must show that the residue of $A$ along each irreducible divisor of $X$ is trivial. We already know that $A$ has zero residue at all irreducible divisors except possibly those appearing in the divisor of $-1$ or $x^2 - 2$.)
(e) Show that for $p \leq \infty$ and $x \in X(\mathbb{Q}_p)$,
\[ \text{inv}_p A(x) = \begin{cases} 0, & \text{if } p \neq 2 \\ 1/2, & \text{if } p = 2. \end{cases} \]
(f) Deduce that $X(A)^{\mathrm{Br}} = \emptyset$ and that $X(\mathbb{Q}) = \emptyset$.

(g) Show that exactly four of the geometric fibers of $X \to \mathbb{P}^1$ are reducible, each consisting of the union of two lines crossing at a point.
(h) Show that each of those lines has self-intersection $-1$.
(i) Deduce that $X^{\text{sep}} := X \times_{\mathbb{Q}} \overline{\mathbb{Q}}$ is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$ blown up at 4 points.
(j) What is Pic $X^{\text{sep}}$?
(k) (Difficult) Show that $\mathrm{Br}\, X/\mathrm{Br}\, \mathbb{Q}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, generated by the image of $A$.

P12. Let $k$ be a field of characteristic not 2. Let $a \in k^\times$.
(a) Show that the affine variety $x^2 - ay^2 = 1$ can be given the structure of an algebraic group $G$.
(b) Show that for every $b \in k^\times$, the affine variety $x^2 - ay^2 = b$ can be given the structure of a $G$-torsor, and that all $G$-torsors over $k$ arise this way.

P13. Let $L/k$ be a finite Galois extension of fields. Let $G = \text{Gal}(L/k)$. View $G$ as a 0-dimensional group scheme over $k$ consisting of one point for each element. Prove that the obvious right action of $G$ on $\text{Spec}\, L$ makes $\text{Spec}\, L$ a $G$-torsor over $\text{Spec}\, k$. 

Let $G$ be a commutative algebraic group over a field $k$, with group law written additively. An extension of the constant group scheme $\mathbb{Z}$ by $G$ (in the category of commutative $k$-group schemes) is a commutative $k$-group scheme $E$ fitting in an exact sequence

$$0 \rightarrow G \rightarrow E \rightarrow \mathbb{Z} \rightarrow 0.$$

A morphism of extensions is a commutative diagram

$$
\begin{array}{cccccc}
0 & \rightarrow & G & \rightarrow & E & \rightarrow \mathbb{Z} & \rightarrow 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & G & \rightarrow & E' & \rightarrow \mathbb{Z} & \rightarrow 0
\end{array}
$$

Given an extension, write $E = \bigsqcup_{n \in \mathbb{Z}} E_n$, where $E_n$ is the inverse image under $E \rightarrow \mathbb{Z}$ of the point corresponding to the integer $n$.

(a) Prove that each $E_n$ is a torsor under $G$.

(b) Prove that there is an equivalence of categories

$$
\{\text{extensions of } \mathbb{Z} \text{ by } G\} \rightarrow \{\text{$k$-torsors under } G\}
$$

$$(0 \rightarrow G \rightarrow E \rightarrow \mathbb{Z} \rightarrow 0) \mapsto E_1,$$

and hence that the set of isomorphism classes of extensions is in bijection with $H^1(k, G)$.

(c) Prove that any extension induces an exact sequence of $G_k$-modules

$$0 \rightarrow G(k^{\text{sep}}) \rightarrow E(k^{\text{sep}}) \rightarrow \mathbb{Z} \rightarrow 0$$

and that the image of $n$ under the coboundary homomorphism $Z = H^0(G_k, \mathbb{Z}) \rightarrow H^1(k, G)$ is the class of the torsor $E_n$.

(Remark: Similarly, a 2-extension

$$0 \rightarrow G \rightarrow E_1 \rightarrow E_0 \rightarrow \mathbb{Z} \rightarrow 0$$

gives rise to a class in $H^2(k, G)$, and so on; this is related to the notion of gerbe.)

Let $k$ be a number field. Let $E$ be an elliptic curve over $k$. Let $m$ be a positive integer. Let $f : E \rightarrow E$ be the multiplication-by-$n$ map.

(a) Explain why $f : E \rightarrow E$ is an $E[n]$-torsor over $E$.

(b) Show that the sets in the resulting partition of $E(k)$ are either empty or cosets of $nE(k)$. (Thus finiteness of the Selmer set $\text{Sel}_f \subseteq H^1(k, E[n])$ implies the weak Mordell–Weil theorem that $E(k)/nE(k)$ is finite.)

(c) Show that the Selmer set $\text{Sel}_f$ is the same as the classically defined $n$-Selmer group of $E$.

Explain why the subset $X(A)^{\text{PGL}}$ cut out by all torsors under all the groups $\text{PGL}_n$ equals the subset $X(A)^{\text{Br}}$.

(An example of E. Victor Flynn) Let $X$ be the smooth projective model of the affine curve $y^2 = (x^2 + 1)(x^4 + 1)$ over $\mathbb{Q}$; this is a genus-2 curve. It turns out that the Jacobian of $X$ is isogenous to a product of two elliptic curves over rank 1, so Chabauty’s method does not apply. For each squarefree integer $d$, let $Y_d$ be the smooth projective model of the affine curve defined by $y^2 = (x^2 + 1)(x^4 + 1)$ and $dz^2 = x^4 + 1$ in $\mathbb{A}^3$ over $\mathbb{Q}$. Let $Y_1 = Y$. Projection (forgetting the $z$-coordinate) induces a morphism $Y_d \rightarrow X$.

(a) Show that $f : Y \rightarrow X$ is a $\mathbb{Z}/2\mathbb{Z}$-torsor over $X$.

(b) Show that the twisted torsors are the curves $Y_d$. 

(3)
(c) Show that $Y_d(A) = \emptyset$ except for $d \in \{1, 2\}$. Thus $\# \text{Sel}_f = 2$.
(d) Let $C_d$ be the smooth projective model of the affine plane curve $dz^2 = x^4 + 1$, so there is also a morphism $Y_d \to C_d$. Assuming that $C_1(Q)$ and $C_2(Q)$ are of size 4 (as could be shown by applying 2-descent to these elliptic curves), compute $Y_1(Q)$ and $Y_2(Q)$.
(e) Finally, compute $X(Q)$.

The online lecture notes at
cover most of the topics presented, and suggest references for further reading. They also implicitly contain solutions to some of the exercises here. (If you get a “Forbidden” error when trying to download this PDF file, try again after a few seconds.)