1) Let p and q be distinct odd primes. Let $U_p = (\mathbb{Z}/p\mathbb{Z})^*$, let $U_q = (\mathbb{Z}/q\mathbb{Z})^*$, and let $U_{pq} = (\mathbb{Z}/pq\mathbb{Z})^*$.

(a) Prove that $U_{pq} \simeq U_p \times U_q$ via the map $\pi(x) = (x \bmod p, x \bmod q)$.

(b) Let $V = \{(1,1),(-1,-1)\} \subset U_p \times U_q$. Prove that the following are coset representatives for V in U:

$$A = \Big\{(a,b) \,\Big|\, 0 \le a \le \frac{p-1}{2},\ \ 0 \le b \le q-1\Big\}$$
$$B = \Big\{(a,b) \,\Big|\, 0 \le a \le p-1,\ \ 0 \le b \le \frac{q-1}{2}\Big\}$$
$$C = \Big\{(a,b) \,\Big|\, a = c \bmod p,\ \ b = c \bmod q,\ \ 0 \le c \le \frac{pq-1}{2}\Big\}$$

(c) Define

$$\alpha = \prod_{(a,b)\in A} (a,b) \qquad \beta = \prod_{(a,b)\in B} (a,b) \qquad \gamma = \prod_{(a,b)\in C} (a,b).$$

Prove that $\pm\alpha = \pm\beta = \pm\gamma$. (This part should use a little bit of group theory.)

(d) Prove the following formulas (p is still an odd prime):

$$(p-1)! \equiv -1 \pmod p$$
$$\Big(\frac{p-1}{2}\Big)!^2 \equiv -(-1)^{\frac{p-1}{2}} \equiv -(-1/p) \pmod p$$

(Recall that $(a/p) = a^{\frac{p-1}{2}}$ is the *Legendre symbol*, introduced in class.) The first of these congruences is called *Wilson's theorem.* You may want to prove the second formula using the first one.

(e) Prove the following formulas (this is just calculation):

$$\alpha = \left((-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{-1}{q}\Big),\ \Big(\frac{-1}{p}\Big)\right)$$
$$\beta = \left(\Big(\frac{-1}{q}\Big),\ (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\Big(\frac{-1}{p}\Big)\right)$$
$$\gamma = \big((-p/q), (-q/p)\big)$$

(f) Compute α/β, β/γ, and α/γ and deduce

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

This is Gauß's "Golden Theorem", quadratic reciprocity. The proof outlined here is due to G. Rousseau [J. Austral. Math. Soc. (Series A) 51 (1991), 423–425], with slight modifications from N. Snyder [math-overflow].

2) Let ω be a primitive third root of unity (e.g., $\omega = e^{2\pi i/3}$).

(a) (deleted)[1]

(b) Prove that $\mathbb{Z}[\omega]$ is a principal ideal domain.

(c) Let $\overline{\omega} = \omega^2 = -\omega - 1$. For any a and b in $\mathbb{Z}$, define $\overline{a + b\omega} = a + b\overline{\omega}$ (this is just complex conjugation) and define $N(x) = x\overline{x}$. Prove that an element x of $\mathbb{Z}[\omega]$ is prime if and only if $N(x)$ is prime.

(d) Show that $x^2 + x + 1 = 0$ has a solution in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 3$ or $p = 3$. (Hint: If $x^2 + x + 1 = 0$ then $x^3 - 1 = 0$. Show that the homomorphism of groups $\varphi(x) = x^3$ from $\mathbb{F}_p$ to itself has nontrivial kernel if and only if $p \equiv 1 \pmod 3$. Be careful about $p = 2$ and $p = 3$.)

(e) Suppose p is a prime in $\mathbb{Z}$. Show that p splits as $q\overline{q}$ in $\mathbb{Z}[\omega]$ if and only if $p \equiv 1 \pmod 3$. Show that p is prime in $\mathbb{Z}[\omega]$ if and only if $p \equiv 2 \pmod 3$. Show that $3\mathbb{Z}[\omega] = (1 - \omega)^2\mathbb{Z}[\omega]$.

[1] The previous statement of this problem was incorrect. Thanks to Daniel for pointing this out.