Math 323: Extra problems of Number-theoretic flavour

1. Find all integer solutions to $y^2 + 1 = x^3$ with $x, y \neq 0$ (Hint: use the ring of Gaussian integers $\mathbb{Z}[i]$).

2. Now we can revisit Pell's equation $x^2 - 2y^2 = \pm 1$.
(a) Show that there is no unit η in $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ such that $1 < \eta < 1 + \sqrt{2}$
(b) Deduce that every positive unit in $\mathbb{Z}[\sqrt{2}]$ is a power of $\epsilon = 1 + \sqrt{2}$

Define the n-th cyclotomic polynomial $\Phi_n(x)$ by: $\Phi_1(x) = x - 1$, and for $n > 1$,

$$\Phi_n(x) = \frac{x^n - 1}{lcm(x^d - 1), 0 < d < n, d|n}.$$

The next few problems are related to the cyclotomic polynomials.

3. (a) Prove that $x^{n-1} + x^{n-2} + ... + x + 1$ is irreducible over $\mathbb{Z}$ if and only if n is prime.
(b) Prove that for a prime p, the cyclotomic polynomial Φ_p is $\Phi_p(x) = x^{p-1} + \cdots + x + 1$.

4. Let φ denote Euler's φ-function.
(a) Prove that $\deg \Phi_n = \varphi(n)$.
(b) Prove the identity $\sum_{d|n} \varphi(d) = n$ where the sum is extended over all the divisors d of n.
(c) Prove that $\Pi_{1 \leq d \leq n, d|n} \Phi_d(x) = \Phi_n(x)$.

5. Prove that the cyclotomic polynomial Φ_5 is irreducible over $\mathbb{F}_p$ iff p is not congruent to $1 \mod 5$ and p^2 is not congruent to $1 \mod 5$ (in the first case it factors into linear factors, and in the second case – into quadratic factors).

Note: we know that it is irreducible over $\mathbb{Z}$, but that does not automatically imply irreducibility $\mod p$ for any prime p! In fact, this polynomial obviously factors into linear factors over $\mathbb{F}_5$.

6. Construct a field with 81 elements.