5 Misc. Ring Tools

2/10: **5.1.** Let M and m denote the lcm and gcd of natural numbers a, b.

(i) Prove that there is an isomorphism of rings

$$\phi : \mathbb{Z}/(a) \times \mathbb{Z}/(b) \to \mathbb{Z}/(M) \times \mathbb{Z}/(m)$$

Hint: Chinese Remainder Theorem.

(ii) Find necessary and sufficient conditions for uniqueness of the ϕ. *Hint*: Do this first when $a = p^c$ and $b = p^d$, where p is prime.

(iii) Prove that the condition you provided for part (ii) is sufficient.

5.2. The Euclidean algorithm for monic polynomials is valid for every commutative ring, but it does not provide a method of obtaining the gcd because the "remainder" may not have a unit as its leading coefficient, so we cannot proceed by induction. But we may get lucky:

(i) Prove that the ideal generated by $X^m - 1$ and $X^n - 1$ in $\mathbb{Z}[X]$ is the principle ideal $(X^d - 1)$, where $d = \gcd(m, n)$.

(ii) Deduce that $\gcd(q^m - 1, q^n - 1) = (q^d - 1)$ for every integer q.

5.3. Let K be the quotient field of a UFD R. If $f \in R[X]$ is a monic polynomial, $c \in K$, and $f(c) = 0$, then $c \in R$.

5.4. State whether true or false. If false, give a counterexample.

(i) If R is a UFD, then $D^{-1}R$ is a UFD.

(ii) Let K be the field of fractions of a PID R. If $R \subset A \subset K$ is a chain of rings, then $A = D^{-1}R$ for some multiplicative subset D of R.

(iii) Same problem as in (ii), except that now R is a UFD.

(iv) Let K be the field of fractions of an integral domain R. If D_1, D_2 are multiplicative subsets of R, then $D_1^{-1}R$ and $D_2^{-1}R$ are subrings of K. If $D_1^{-1}R = D_2^{-1}R$, then $D_1 = D_2$.

5.5. Let $f \in \mathbb{Z}[X]$ be a polynomial with content 1. Let p be prime and let $\bar{f}$ denote the image of f in $\mathbb{F}_p[X]$. If $\deg(f) = \deg(\bar{f})$ and $\bar{f}$ is irreducible, show that f is irreducible in $\mathbb{Z}[X]$.

5.6. If R is a (commutative) ring of characteristic p, where p is prime, show that $(a + b)^p = a^p + b^p$.