Trento Scholarship
for Master's degree in Mathematics,
Major in Coding Theory and Cryptography

July, 22, 2016

Solve the largest possible number of the following exercises.
The reference book is Lindsay N. Childs, *A concrete introduction to higher algebra* (Undergraduate Texts in Mathematics) Third edition, Springer, 2008.

1. (10 pts) Section IV - Polynomials

   Let $f(x) = x^2 + bx + 1 \in \mathbb{R}[x]$. For each b in $\mathbb{R}$, factor $f(x)$ into a product of irreducible polynomials in $\mathbb{R}[x]$.

2. (10 pts) Section III - Congruences and groups

   Find all solutions of
   $$\begin{cases} x \equiv 2 & \mod 12 \\ x \equiv 8 & \mod 10 \\ x \equiv 10 & \mod 14 \end{cases}$$
   Write the set of solutions, if any, as the solutions to a single congruence.

3. (20 pts) Section III - Congruences and groups

   Let $m = 252601$. Suppose we discover that

   - $3^{126300} \equiv 67772 \mod 252601$
   - $3^{252600} \equiv 1 \mod 252601$.

   Is then 252601 prime? composite? Or can we not decide for sure from the information given?

Prove the following theorems

4. (10 pts) Proposition 8, p. 115:

   If $d = (a, m)$, then the general solution in $\mathbb{Z}/m\mathbb{Z}$ of $[a]X = [0]$ is
   $$X = [\frac{m}{d}k], \text{ for } k = 0, 1, ..., d-1.$$

5. (10 pts) Proposition 18, p. 142:

   Let R be a commutative ring with identity 1_R.
   The function $f : \mathbb{Z} \to R$ defined by $f(n) = n \cdot 1_R$ is a homomorphism, and is the only ring homomorphism from $\mathbb{Z}$ to R.

6. (20 pts)*Fundamental Theorem of Algebra* (Theorem 6, p. 329):

   Every polynomial $p(x)$ in $\mathbb{C}[x]$ of degree ≥ 1 has a root in $\mathbb{C}$.

7. (10 pts) *Euler's Lemma*(Theorem 5, p. 439):

   Let p be an odd prime. If $(a, p) = 1$, then

$$(\frac{a}{p}) \equiv a^{(p-1)/2} \mod p.$$

8. (10 pts) *The Chinese Remainder Theorem*(Theorem 7, p. 364):

   Let F be a field. Let $a_1(x), ..., a_d(x)$ be arbitrary polynomials, and $m_1(x), ..., m_d(x)$ be pairwise coprime polynomials in $F[x]$. Then there exists a polynomial $f(x)$ in $F[x]$ such that

$$f(x) \equiv a_1(x) \mod (m_1(x))$$

$$\vdots$$

$$f(x) \equiv a_d(x) \mod (m_d(x)).$$

   If $f_1(x)$ and $f_2(x)$ are two solutions, then

$$f_1(x) \equiv f_2(x); \mod m_1(x) \cdots m_d(x).$$