MAT 312/AMS 351: Applied Algebra
Solutions to Problem Set 1 (18pts)

1.1 2; 3pts *Find* $\gcd(6,14,21)$ *and express it in the form* $6\alpha+14\beta+21\gamma$ *for some* $\alpha,\beta,\gamma\in\mathbb{Z}$.

We use Euclid's algorithm, first with non-matrix version and then matrix version.

Non-matrix version. Note that $\gcd(6,14,21)=\gcd(\gcd(6,14),21)$. We first apply Euclid's algorithm with $(6,14)$:

$$(1):\ 14 = 2\cdot\mathbf{6}+\mathbf{2} \qquad\qquad \gcd(6,14) = \mathbf{2} \overset{(1)}{=\!=} 14 - 2\cdot\mathbf{6}.$$
$$(2):\ \mathbf{6} = 3\cdot\mathbf{2}+\mathbf{0}$$

We next apply Euclid's algorithm with $(\gcd(6,14),21)=(2,21)$:

$$(3):\ 21 = 10\cdot\mathbf{2}+\mathbf{1} \qquad \gcd(2,21) = \mathbf{1} \overset{(3)}{=\!=} 21 - 10\cdot\mathbf{2}$$
$$(4):\ \mathbf{2} = 2\cdot\mathbf{1}+\mathbf{0} \qquad = 21 - 10\cdot(14-2\cdot\mathbf{6}) = 20\cdot6-10\cdot14+1\cdot21.$$

Thus, $\gcd(6,14,21) = \boxed{1 = 20\cdot6+(-10)\cdot14+1\cdot21}$

Matrix version:

$$\left(\begin{array}{ccc|c} 1 & 0 & 0 & 6\\ 0 & 1 & 0 & 14\\ 0 & 0 & 1 & 21\end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 0 & 6\\ -2 & 1 & 0 & 2\\ -3 & 0 & 1 & 3\end{array}\right) \longrightarrow \left(\begin{array}{ccc|c} 7 & -3 & 0 & 0\\ -2 & 1 & 0 & 2\\ -1 & -1 & 1 & 1\end{array}\right).$$

The second matrix is obtained from the first by subtracting the first row (which has the smallest last entry 6) times 2 from the second row (largest multiple of 6 dividing the last entry in the second row 14) and times 3 from the third row. The third matrix is obtained from the second by subtracting the second row (which has the smallest last entry 2) times 3 from the first row (largest multiple of 2 dividing the last entry in the first row 6) and times 1 from the third row. Since the last entry in the third row of the third matrix divides all other entries, this entries is $\gcd(6,14,21)$ and this row gives

$$\gcd(6,14,21) = \boxed{1 = (-1)\cdot6+(-1)\cdot14+1\cdot21}$$

The computation above is a shorthand for

$$\begin{pmatrix} 1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix} 6\\ 14\\ 21\end{pmatrix} = \begin{pmatrix} 6\\ 14\\ 21\end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0\\ -2 & 1 & 0\\ -3 & 0 & 1\end{pmatrix}\begin{pmatrix} 6\\ 14\\ 21\end{pmatrix} = \begin{pmatrix} 6\\ 2\\ 3\end{pmatrix}$$
$$\longrightarrow \begin{pmatrix} 7 & -3 & 0\\ -2 & 1 & 0\\ -1 & -1 & 1\end{pmatrix}\begin{pmatrix} 6\\ 14\\ 21\end{pmatrix} = \begin{pmatrix} 0\\ 2\\ 1\end{pmatrix}.$$

1.1 6; 3pts *Suppose that* $\gcd(a,c)=1$ *and* $\gcd(b,c)=1$. *Show that* $\gcd(ab,c)=1$.

By Corollary 1.1.3 (the main theorem of the chapter, stated as Theorem 1 in every lecture), there exist $\alpha,\beta,\gamma,\gamma'\in\mathbb{Z}$ such that

$$\alpha a+\gamma c=\gcd(a,c)=1 \qquad \text{and} \qquad \beta b+\gamma' c=\gcd(b,c)=1.$$

Multiplying the two equations together, we obtain

$$\alpha\beta(ab)+\big(\alpha\gamma' a+\beta\gamma b+\gamma\gamma' c\big)c=1.$$

Since $\gcd(ab,c)$ divides ab and c, it divides each term on LHS above and thus their sum 1. Since $\gcd(ab,c)\in\mathbb{Z}^+$ divides 1, it equals 1.

1.2 2; 3pts *Show that* $\sum_{i=1}^{n} i^2=\frac{n(n+1)(2n+1)}{6}$ *for all* $n\in\mathbb{N}$.

We use induction. Since

$$\sum_{i=1}^{1} i^2=1=\frac{1(1+1)(2\cdot 1+1)}{6},$$

the claim holds in the base $n=1$ case. If the claim holds for some $n\in\mathbb{N}$, then

$$\begin{aligned}\sum_{i=1}^{n+1} i^2=\sum_{i=1}^{n} i^2+(n+1)^2=\frac{n(n+1)(2n+1)}{6}+(n+1)^2&=\frac{(n+1)(n(2n+1)+6(n+1))}{6}\\&=\frac{(n+1)(2n^2+7n+6)}{6}=\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6},\end{aligned}$$

i.e. the claim holds for $n+1$. This completes the proof.

1.2 3; 3pts *Each term in the* Fibonacci sequence $1,1,2,3,5,\ldots$ *is the sum of the two preceding terms. Show that every two successive terms in the sequence are relatively prime.*

The Fibonacci sequence $a_0,a_1,a_2,\ldots$ is defined recursively by

$$a_0=1, \qquad a_1=1, \qquad a_{n+2}=a_n+a_{n+1} \quad \forall\, n\ge 0.$$

We need to show that $\gcd(a_n,a_{n+1})=1$ for all $n\ge 0$. We use induction. Since

$$\gcd\big(a_0,a_{0+1}\big)=\gcd(1,1)=1,$$

the claim holds in the base $n=0$ case. If the claim holds for some $n\ge 0$, then

$$\gcd\big(a_{n+1},a_{(n+1)+1}\big)=\gcd\big(a_{n+1},a_n+a_{n+1}\big)=\gcd\big(a_{n+1},a_n\big)=1;$$

the middle equality above holds by Lemma 1.1.4. Thus, the claim holds for $n+1$. This completes the proof.

1.3 2; 3pts *Show that it is enough to strike out all multiples of primes not exceeding $\sqrt{n}$ when using the sieve method to find all primes not exceeding n.*

Suppose $2 \le m \le n$ and no prime $p \le \sqrt{n}$ divides m; we show that m is prime and thus should not be struck out. By Theorem 1.3.3 (Unique Factorization for $\mathbb{Z}^+$), $m = p_1 p_2 \ldots p_r$ for some $r \ge 1$ and primes $p_1, p_2, \ldots, p_r$. Since no prime $p \le \sqrt{n}$ divides m, $p_i > \sqrt{n}$ for all $i = 1, 2, \ldots, r$. If $r \ge 2$, then

$$m \ge p_1 p_2 > \sqrt{n} \cdot \sqrt{n} = n,$$

contrary to the assumption that $m \le n$. Thus, $m = p_1$ is prime.

1.3 7; 3pts *Suppose $2^n + 1$ is prime for some $n \in \mathbb{Z}^+$. Show that $n = 2^k$ for some $k \in \mathbb{Z}^{\ge 0}$.*

Suppose not. By Theorem 1.3.3 (Unique Factorization for $\mathbb{Z}^+$), a (prime) odd integer $p \ge 3$ then divides n, i.e. $n = kp$ for some $k \in \mathbb{Z}^+$ with $k < n$. Since p is odd,

$$2^n + 1 = (2^k)^p + 1^p = \big(2^k + 1\big)\big((2^k)^{p-1} 1^0 - (2^k)^{p-2} 1^1 - + \ldots - (2^k)^1 1^{p-2} + (2^k)^0 1^{p-1}\big).$$

Thus, the integer $2^k + 1$ divides $2^n + 1$. Since $1 < 2^k + 1 < 2^n + 1$, this contradicts to $2^n + 1$ being prime. Thus, $n = 2^k$ for some $k \in \mathbb{Z}^{\ge 0}$.