DISCRETE MATHEMATICS

HOMEWORK 3

(1) Use the Euclidean algorithm to compute the gcd of 213 and 1820, and to write this gcd as a linear combination of these integers.

$$\begin{aligned}
1820 &= 8 \cdot 213 + 116 \\
213 &= 1 \cdot 116 + 97 \\
116 &= 1 \cdot 97 + 19 \\
97 &= 5 \cdot 19 + 2 \\
19 &= 9 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

Thus $\gcd(1820, 213) = 1$.

Working backwards we now get

$$\begin{aligned}
1 &= 19 - 9 \cdot 2 \\
&= 19 - 9 \cdot (97 - 5 \cdot 19) = 46 \cdot 19 - 9 \cdot 97 \\
&= 46 \cdot (116 - 97) - 9 \cdot 97 = 46 \cdot 116 - 55 \cdot 97 \\
&= 46 \cdot 116 - 55 \cdot (213 - 116) = 101 \cdot 116 - 55 \cdot 213 \\
&= 101 \cdot (1820 - 8 \cdot 213) - 55 \cdot 213 = 101 \cdot 1820 - 863 \cdot 213
\end{aligned}$$

(2) Show that $\gcd(5n + 3, 7n + 4) = 1$, and write 1 as a linear combination of these integers.

$$\begin{aligned}
7n + 4 &= 1(5n + 3) + 2n + 1 \\
5n + 3 &= 2(2n + 1) + n + 1 \\
2n + 1 &= 1(n + 1) + n \\
n + 1 &= 1 \cdot n + 1 \\
n &= n \cdot 1
\end{aligned}$$

Working backwards we find

$$\begin{aligned}
1 &= (n + 1) - n \\
&= 2(n + 1) - (2n + 1) \\
&= 2(5n + 3 - 2(2n + 1)) - (2n + 1) = 2(5n + 3) - 5(2n + 1)
\end{aligned}$$

(3) Show that $2^{104} \equiv 16 \bmod 101$. (Hint: 101 is a prime; Fermat's Little Theorem).

Fermat's Little Theorem says that $2^{101} \equiv 2 \bmod 101$. Multiplication by $2^3 = 8$ gives $2^{104} \equiv 16 \bmod 101$.

(4) Check whether the ISBN $0 - 387 - 90533 - 2$ is correct.

Multiplying the digits by $1, 2, \ldots, 10$ from the left, reducing mod 11, and adding gives $0 + 6 + 24 + 28 + 45 + 0 + 35 + 24 + 27 + 20 \equiv 6 + 2 + 6 + 1 + 2 + 2 + 5 - 2 \equiv 0 \bmod 11$. Thus the ISBN is valid.

(5) Compute the check digit $*$ of the book number $3 - 540 - 90279 - *$

We find $3+10+12+0+45+0+14+56+81-* \equiv 3-1+1+1+3+1+4-* \equiv 1 - * \bmod 11$; since the result must be 0 mod 11, the check digit is 1.