Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. The Caeser cipher.

    (a) Encrypt the message "exchange all assets" using a Caesar cipher with a forward shift of 5 characters.

    (b) Decrypt the following message, which has been encoded with a Caesar cipher.

    ```
    DPYLA OLTVU LFAVT VYYVD
    ```

2. An Improved Caeser. Consider the following variant on the Caeser cipher. Two integer keys k_1 and k_2 are selected. To encode a message, the first letter is shifted forward by k_1 letters. The second letter is shifted forward by k_2 letters. The third letter is shifted forward by k_1 letters, the forth by k_2 letters, and so on until the end of the message.

    (a) How many improved Caeser ciphers are there?

    (b) Describe an efficient technique to break the improved Caeser cipher. (By efficient, we want something which is faster than trying all possible improved Caeser ciphers.)

    (c) The following excerpt has been encrypted with an improved Caeser cipher.

    ```
    RWCHF XNXQA WXLVF TPTGC RWCWY GZDPD DCYEJ TQFSP PPLIG CCSQW
    CWYHZ TCCFT PTQTT TPPJS YNQPL SUXJA PTKPG CQTTT PPJBM GCLCI
    FPRRY BCQWG YXJUP DKGMB CWYKC TQRYE CSRWG HKXQU MGRJL TMUAD
    SGQTL DMCCX QPJAM LCSRD EDMCZ DYGBI FTQWG EMGAD KTYHF DPTDG
    MBFTP HFTGH YEPXQ DLCML RWCEY HQTLV CGQEP DZPZA WHNTL SRWCA
    MCEQJ PXXLV BPWHJ DMZGC EDSID GMBSC BTPIF TYLLX LVQPR KCHSK
    GJQPL SRWCQ CPSIG USAAX RNYCB XLHUT YGGCE IFXLZ MURTL SYNQD
    DIFXQ HMGRD DEYHR XKTUT EDMJR TTTPN BPWXL PZDYI YCBGC FSTQI
    RWCBR DADKT YHFDP TGIQD MIFTQ IFTKL CAGTR TLHRT NHDGM BRWCH
    FXNPL SRTJA RWCBF DUHNA CCBXB IFTAX RNGHY CBWML KJAWZ TRICG
    RWCWM ICADP PTGHF TPTRW YCYCW LFTPT CAQTG CCJPD NTYCB WMLAD
    MAGIG HYCBL FPRUP DXTLR MCRXL TLIQD DXATA GCPKI FTPTY GCPLS
    UWYIY IGBCL CPPTF PTXLV APTDP IGCEP ZDSIR WCRMJ LIPNY CBHYX
    JXLVR DRWCX QAYCB HGCRW CQYNR WGHRG YCOJG AGOCH RWCB
    ```

    What are the first 11 words of this excerpt?

3. [JJJ 1.{9,10}.c] Let $d = \gcd(16261, 85652)$. Use the extended Euclidean algorithm to find integers u and v such that $16261u + 85652v = d$.

4. Let a, b, and c be integers such that $a \mid b$ and $a \mid c$. Prove that $a \mid (b + c)$ and $a \mid (b - c)$.

5. **[Challenge]** Let $a_1, a_2, \ldots, a_k$ be integers, not all of which are zero. We define $\gcd(a_1, \ldots, a_k)$ to be the largest integer that divides every integer in $\{a_1, \ldots, a_k\}$. Show that there exist integers $u_1, \ldots, u_k$ such that $u_1a_1 + u_2a_2 + \cdots + u_ka_k = d$.