سری دوم تمرینات ریاضیات رمزنگاری

۱- مسائل ۱۱، ۱۲، ۱۵ و ۱٦ از بخش ۳.٤ کتاب

۲- نشان دهید دنباله $\{6k+5\}_{k=0}^{\infty}$ حاوی بینهایت عدد اول است.

۳- نشان دهید اگر gcd(a,b)=1 باشد آنگاه gcd(a-b,a+b)=1 or 2. چه وقت gcd(a-b,a+b)=2 است؟

٤- اگر $a+b \neq 0$ و $\gcd(a,b)=1$ و p یک عدد اول فرد باشد. نشان دهید که:

$$\gcd\left(a+b, \frac{a^p+b^p}{a+b}\right) = 1 \text{ or } p$$

۵- بررسی و تعیین پیچیدگی روش Trial Division در تجزیه اعداد.

٦- نشان دهید که هر عدد کامل زوج بصورت $2^{n-1}.M(n)$ است که در آن M(n) یک عدد اول مرسن است.

۷- اگر a و b دو عدد صحیح غیرصفر باشند و (x_0,y_0) جوابی از معادله ax+by=c باشد. نشان دهید دیگر جوابهای معادله بصورت زیر است:

$$x = x_0 + \frac{b}{d}t \qquad y = y_0 - \frac{a}{d}t$$

که در آن t یک عدد صحیح دلخواه و d=gcd(a,b) است.

۸- اگر gcd(a,m)|c در این صورت معادله $ax \equiv c \pmod m$ دارای تعداد متناهی جواب متمایز به پیمانه m است که از رابطه زیر بدست می آیند:

$$x = x_0 + \frac{t.m}{\gcd(a,m)} \pmod m \quad ; t = 1,2,\dots,\gcd(a,m)$$

تاریخ تحویل: دوشنبه ۱۳۸۷/۸/٦ (چون شنبه تعطیل است.)