Q.ing 4

6) $a \mid c \Rightarrow \frac{c}{a} = k$
$b \mid d \Rightarrow \frac{d}{b} = l$
} where $k \& l$ are integers

$ab \mid cd \Rightarrow \frac{cd}{ab} = \frac{c}{a} \cdot \frac{d}{b} = \underline{k \cdot l}$

if $k \& l$ are integers, then $a \mid c$ & $b \mid d$, and also $ab \mid cd$

13d) $C \equiv 2a + 3b \pmod{13}$

$C \bmod 13 = 2(4) + 3(9) \bmod 13$

$C = 8 + 27 \bmod 13$

$\underline{C = 9}$

38) if n is odd:

$n = 2a+1$

$n^2 = (2a+1)^2 = 4a^2 + 4a + 1$

$= 4(a^2+a) + 1$

$n^2 \equiv 4(a^2+a) + 1 \pmod 4$

$n^2 \equiv 0 + 1 \pmod 4 \equiv 1 \pmod 4$

if n is even:

$n = 2k$

$n^2 = 4k^2$

$n^2 \equiv (2k)^2$

$n^2 \equiv 4k^2$

$4k^2 \equiv 0 \pmod 4$

14d) $7(11) + 3(3) = (77+9) \bmod 19$

$= \underline{\underline{10}}$

33 b) $(3^4 \bmod 17)^2 \bmod 11$

$= (81 \bmod 17)^2 \bmod 11$

$= 13^2 \bmod 11$

$= \underline{\underline{4}}$

Seksjon 4.2

3b

512	256	128	64	32	16	8	4	2	1
1	0	0	0	0	0	0	0	0	1

$= 1 \cdot 1$, $1 \cdot 512$ $\Rightarrow = \underline{\underline{513}}$

7b $(1\,3\,5\,A\,B)_{16} = B \cdot 1$, $A \cdot 16$, $5 \cdot 16^2$, $3 \cdot 16^3$, $1 \cdot 16^4$ $\Rightarrow = \underline{\underline{79\,275}}$

24) a) Sum =

$$\begin{array}{r} {\scriptstyle 1\ 1} \\ 1\,A\,E \\ B\,B\,C \\ \hline D\,B\,A \end{array}$$

$= \underline{\underline{D6A}}$

Multiplication:

$$\begin{array}{r} {\scriptstyle 2\ 1} \\ 1\,A\,E \\ B\,B\,C \\ \hline 1\,4\,2\,8 \\ 1\,2\,7\,A \\ \hline 1\,2\,7\,A \\ \hline 1\,3\,B\,5\,C\,8 \end{array}$$

Session 4.3

6) 157

12) $m < n$

$$n! + m = m + (1 \cdot 2 \cdot \ldots \cdot m \cdot \ldots \cdot n)$$
$$= m\left(1 + \frac{n!}{m}\right)$$

Since $\frac{n!}{m}$ is an integer, $m(1+n)$ will be a composite integer. Since m is bound by n, this gives $(n-1)$ consecutive composites. Since $n \mid (n!)$, n is also a composite. This gives n consecutive composites.

33 c) $1331 - 1001 = 330$

$1001 - 330 \cdot 3 = 11$

d) $54321 - 4(12345) = 4941$

$12345 - 2(4941) = 2463$

$4941 - 2(2463) = 15$

$2463 - 164(15) = 3$

39 e) $213 = 1 \cdot 117 + 96$
$117 = 96 + 21$
$96 = 4 \cdot 21 + 12$
$21 = 12 + 9$
$12 = 9 + 3$
$9 = 3 \cdot 3$

$3 = 12 - 9$
$= 12 - (21 - 12)$
$= 2 \cdot 12 - 21$

$12 = 96 - 4 \cdot 21$
$3 = 2(96 - 4 \cdot 21) - 21$
$= 2 \cdot 96 - 9 \cdot 21$
$21 = 117 - 96$
$3 = 2 \cdot 96 - 9 \cdot (117 - 96)$
$= 11 \cdot 96 - 9 \cdot 117$

$3 = 11 \cdot (213 - 117) - 9 \cdot 117$

$3 = 11 \cdot 213 - 20 \cdot 117$

(49) By definition one of the three consecutive integers are divisible by three, and at least one of them are divisible by two.
this means the product of three consecutive integers is divisible by 6.

SECTION 4.4

5b) 19 mod 141

$\gcd(141, 19)$: $141 = 19 \cdot 7 + 8$
$19 = 8 \cdot 2 + 3$
$8 = 3 \cdot 2 + 2$
$3 = 2 + 1$
$2 = 1 \cdot 2$

$\gcd(141, 19) = 1$

$1 = 3 - 2$

$2 = 8 - 3 \cdot 2$

$3 = 19 - 8 \cdot 2$

$8 = 141 - 19 \cdot 7$

$1 = 3 - (8 - 3 \cdot 2)$
$1 = 3 \cdot 3 - 8$

$1 = 3(19 - 8 \cdot 2) - 8$
$= 3 \cdot 19 - 7 \cdot 8$

$1 = 3 \cdot 19 - 7(141 - 19 \cdot 7)$
$= 3 \cdot 19 - 7 \cdot 141 + 49 \cdot 19$
$1 = 52 \cdot 19 - 7 \cdot 141$

Bézout coeffs: 52, -7

inverse of 19 mod 141 = 52

5c) 55 mod 89 :

$$89 = 1 \cdot 55 + 34$$
$$55 = 1 \cdot 34 + 21$$
$$34 = 1 \cdot 21 + 13$$
$$21 = 1 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$

$1 = 3 - 2$

$1 = 2 \cdot 3 - 5$

$1 = 2(8-5) + 5$

$1 = 2 \cdot 8 - 3 \cdot 5$

$1 = 2 \cdot 8 - 3(13-8)$

$1 = 5 \cdot 8 - 3 \cdot 13$

$1 = 5 \cdot 21 - 8 \cdot 13$

$1 = 13 \cdot 21 - 8 \cdot 34$

$1 = 13 \cdot 55 - 21 \cdot 34$

$1 = 13 \cdot 55 - 21 \cdot 89 + 21 \cdot 55$

$1 = 34 \cdot 55 - 21 \cdot 89$

$2 = 5 - 3$

$3 = 8 - 5$

$5 = 13 - 8$

$8 = 21 - 13$

$13 = 34 - 21$

$21 = 55 - 34$

$34 = 89 - 55$

Bézout : 34, -21

inverse : 34

8) If there is a inverse of $x \bmod n$, it gives us a y so that $xy \bmod n = 1$

$$xy = kn + 1$$

$$xy - kn = 1$$

For any common divisor of x and n, $c \mid (xy - kn)$ which gives $c \mid 1$.

This shows that only when $c = 1$, which is the common divisor, x $\bmod n$ has a inverse.

11a) $19x \equiv 4 \pmod{141}$

$19 \cdot 52 \equiv 52 \cdot 4 \pmod{141}$

$988 \equiv 1 \pmod{141}$

$208 \equiv 67 \pmod{141}$

$x \equiv 208 \equiv 67 \pmod{141}$

$19(67) = 1273 \equiv 4 \pmod{141}$ $\quad x = 67$

11b) $55x \equiv 34 \pmod{89}$

$55 \cdot 34 = 34^2 \pmod{89}$

$55 \cdot 34 \equiv 1 \pmod{89}$

$34^2 \equiv 88 \pmod{89}$

$x \equiv 34^2 \equiv 88 \pmod{89}$

$55(88) = 4840 \equiv 34 \pmod{89}$

$x = 88$