Solutions of homework problems.
Math 113
Vera Serganova

20 (1.2) Write $a = 2k + 1$. Then

$$a^2 - 1 = (a - 1)(a + 1) = 2k(2k + 2) = 4k(k + 1).$$

Note that either $2|k$ or $2|k + 1$. Hence $8|4k(k + 1)$.

36 (1.2) Use $(a, b) = (a, b - aq)$ to get

$$\left(n + 1, n^2 - n + 1\right) = \left(n + 1, n^2 - n + 1 - (n + 1)(n - 2)\right) = (n + 1, 3).$$

Now $(n + 1, 3)$ is either 1 or 3.

32(1.2) If $d_1, \ldots, d_k$ are digits of n, n can be written in the form

$$d_1 10^{k-1} + d_2 10^{k-2} + \cdots + d_k.$$

Define $S = d_1 + \cdots + d_k$. Let

$$\Delta = n - S = d_1\left(10^{k-1} - 1\right) + d_2\left(10^{k-2} - 1\right) + \ldots. + d_{k-1}(10 - 1).$$

Note that $10^s - 1 = 99\ldots9 = 3(33\ldots3)$ is divisible by 3 for all s. Hence $3|\Delta$. If $3|S$, then $3|(S + \Delta = n)$. If $3|n$, then $3|(n - \Delta = S)$.

11(1.4) Let us assume that there only finitely many prime numbers of the form $4k + 3$. Denote them by $p_1, \ldots, p_n$. Note that p_1^2 will be of the form $4k + 1$, and therefore $p_1^2 \ldots p_n^2$ is of the form $4k + 1$. Let $m = p_1^1 \ldots p_n^2 + 2$. Then m is of the form $4k + 3$, therefore it has at least one prime factor p of the form $4k + 3$. But p_i does not divide m for $i = 1, \ldots, n$, therefore $p \neq p_i$. This contradicts the assumption that $p_1, \ldots, p_n$ are ALL primes of the form $4k + 3$.

12(1.4) At least one of the numbers n, $n + 2$ and $n + 4$ is divisible by 3. If they are all prime, one of them is 3, which is possible only if $n = 3$.

14(1.4) Induction on n. If $n = 1$, $p_1 = 2 \leq 2^{2^{n-1}} = 2$. If $p_1, \ldots, p_n$ are first n primes. Then

$$p_{n+1} \leq p_1 \ldots p_n + 1.$$

By induction assumption $p_k \leq 2^{2^{k-1}}$ for all $k \leq n$. Therefore

$$p_{n+1} \leq 2^{2^0+2^1+2^2+\cdots+2^{n-1}} + 1 = 2^{2^n-1} + 1 = \frac{1}{2}2^n + 1 \leq 2^{2^n}.$$

30(2.1) We have to show that $30|a^5 - a$. It is sufficient to show that 2,3 and 5 divide $a^5 - a$. $5|a^5 - a$ by Fermat's little Theorem. To prove that 2 and 3 divide $a^5 - a$, factor

$$a^5 - a = a\left(a^4 - 1\right) = a\left(a^2 - 1\right)\left(a^2 + 1\right) = a(a - 1)(a + 1)\left(a^2 + 1\right).$$

Now $2|a - 1$ or $2|a$, 3 divides one of three consequtive numbers $a - 1, a, a + 1$.

13(2.3) Assume that $ax = 0$ has a non-zero solution $x = b$. Then $n|ab$ but n does not divide b. Therefore $d = (n, b) > 1$. But the equation $ax = 1$ has a solution in

$\mathbb{Z}_n$ if and only if $ac = 1 + nk$, for some $c, k \in \mathbb{Z}$. Therefore $(a, n) = 1$. Thus, the equation $ax = 1$ does not have solutions in $\mathbb{Z}_n$.

Now assume that $ax = 1$ has a solution $x = c$. Multiply by c the equation $ax = 0$. Get $c\,(ax) = 0$, $ca = 1$ implies $x = 0$.

6(3.1) No, not closed under addition.

20(3.1) Note $a \oplus 1 = a$. So $1 = 0_R$. Also $a \circ 2 = 2 \circ a = a$, therefore $2 = 1_R$. The ring has identity and commutative. The condition

$$a \circ b = 0_R$$

can be translated in usual language

$$ab - (a + b) + 2 = 1.$$

Therefore $ab - a - b + 1 = (a - 1)\,(b - 1) = 0$. Hence $a = 1 = 0_R$ or $b = 1 = 0_R$.

29(3.1) Both are wrong, because $(1_R, 0_S)\,(0_R, 1_S) = (0_R, 0_S) = 0_{R\times S}$, zero product rule does not work.

5(3.2) (a) Yes, if $a, b \in S \cap T$, then $a - b \in S \cap T$ and $ab \in S \cap T$. (b) not true. For example, consider two subrings T and S in $\mathbb{Z}$, S being the subset of even numbers, T being the subset of numbers divisible by 3.

22(3.2)

$$a + a = (a + a)^2 = a^2 + a^2 + a^2 + a^2 = (a + a) + (a + a) \Rightarrow a + a = 0_R$$

$$a+b = (a + b)^2 = a^2+ab+ba+b^2 = (a + b)+ab+ba \Rightarrow ab+ba = 0_R, (ab + ab = 0_R) \Rightarrow ab = ba.$$

30(3.2) Suppose $a^n = 0_R$ for some $a \neq 0_R$ and $n > 1$. Choose the minimal n such that $a^n = 0_R$. If n is even, $n = 2k$, and $x = a^k$ is a nonzero solution for $x^2 = 0_R$. If n is odd, then $n = 2k + 1$, and $x = a^{k+1}$ is a nonzero solution for $x^2 = 0_R$. If $x^2 = 0_R$ does not have nonzero solutions, R should not have nonzero nilpotents elements. If $x^2 = 0_R$ has a nonzero solution, this solution is a nilpotent element.